

FIG. 1

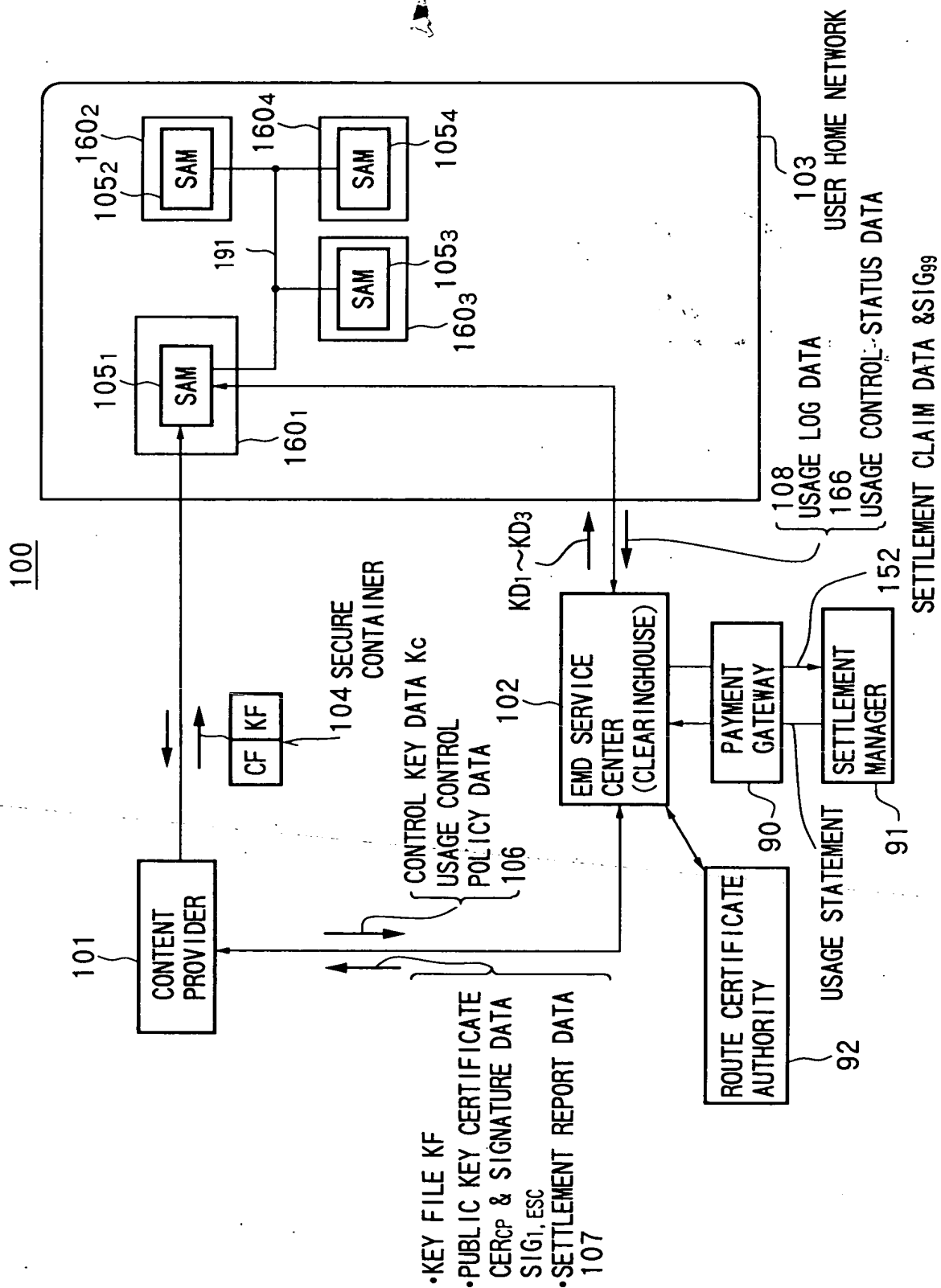


FIG.2

CONCEPT OF SECURE CONTAINER OF PRESENT INVENTION

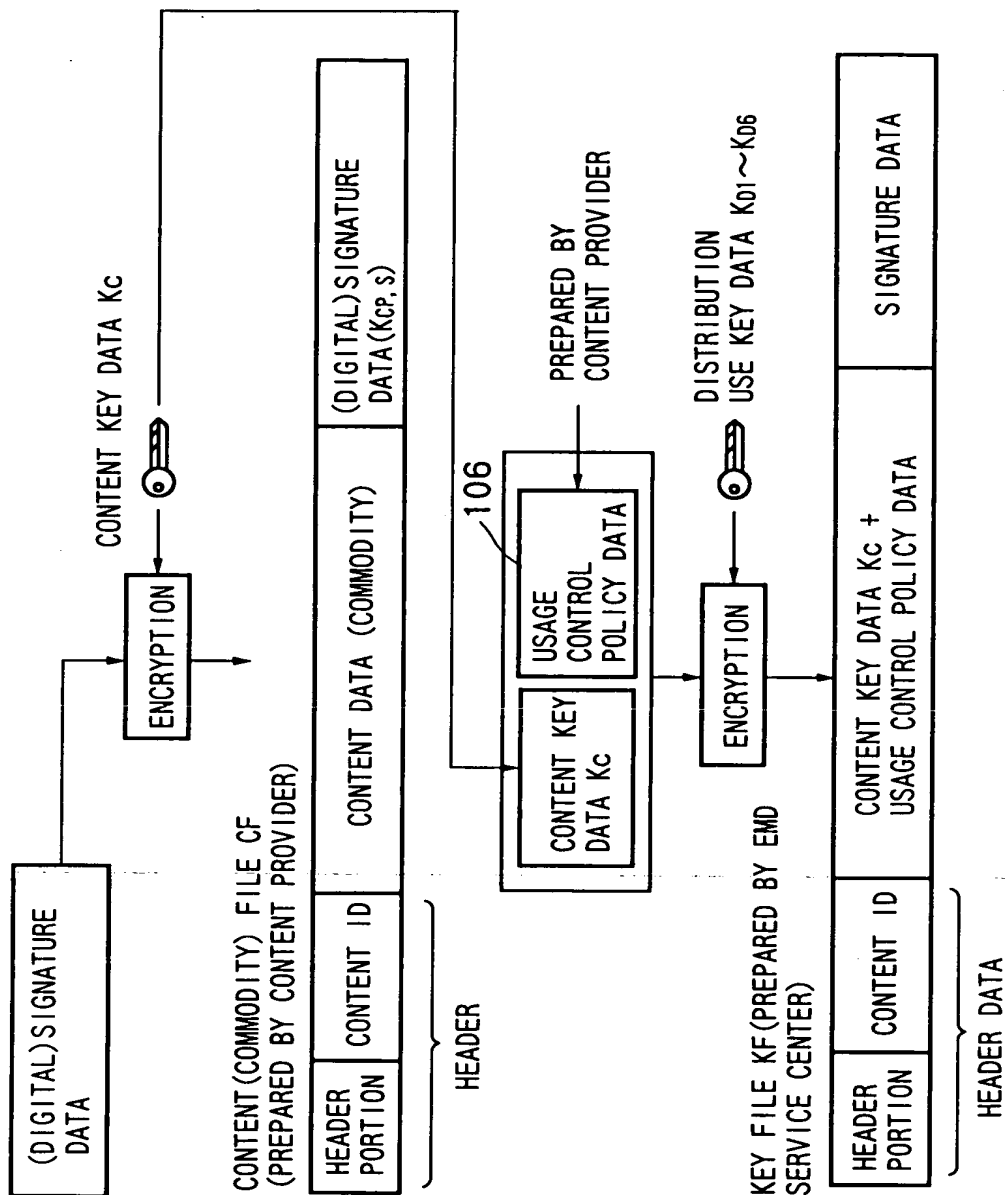
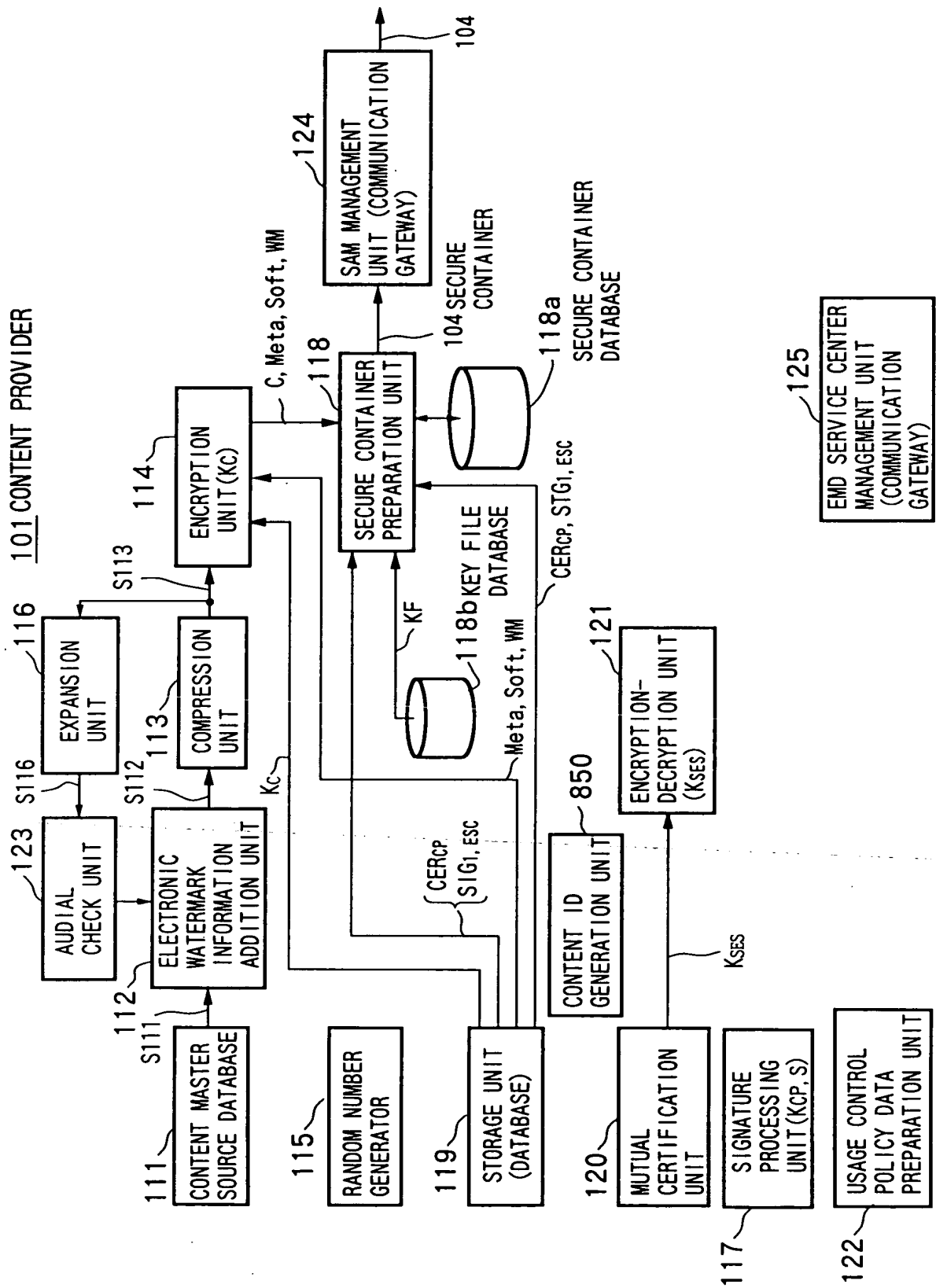
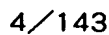


FIG. 3



101 CONTENT PROVIDER



104 SECURE CONTAINER

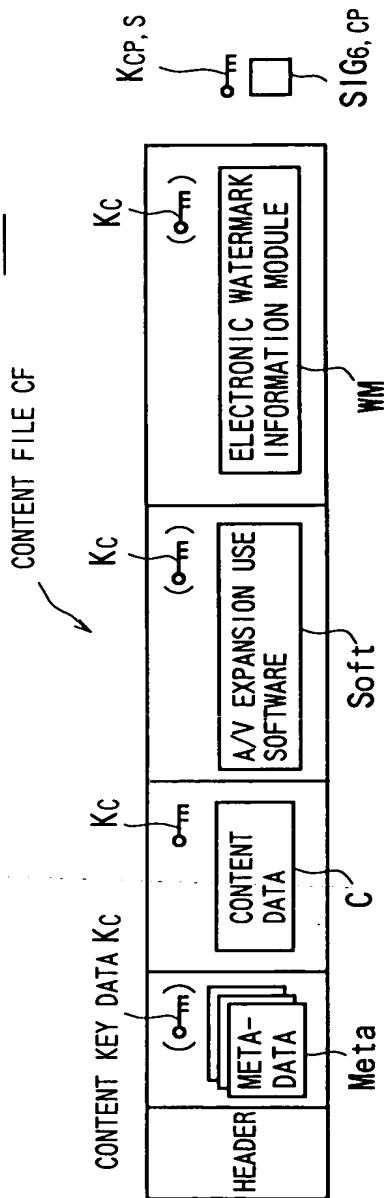


FIG. 5A

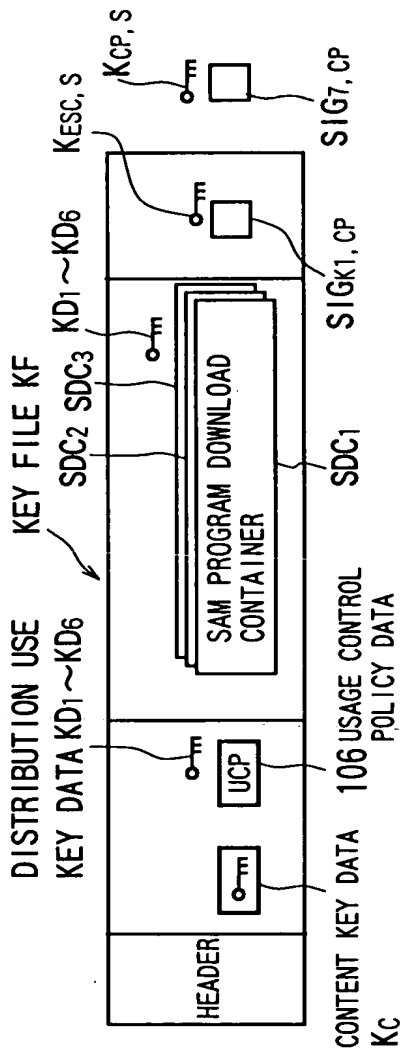


FIG. 5B

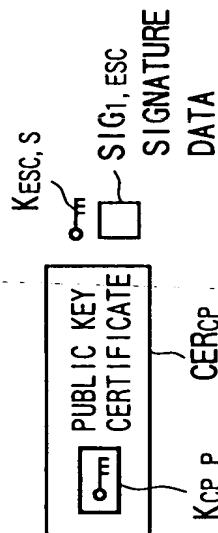
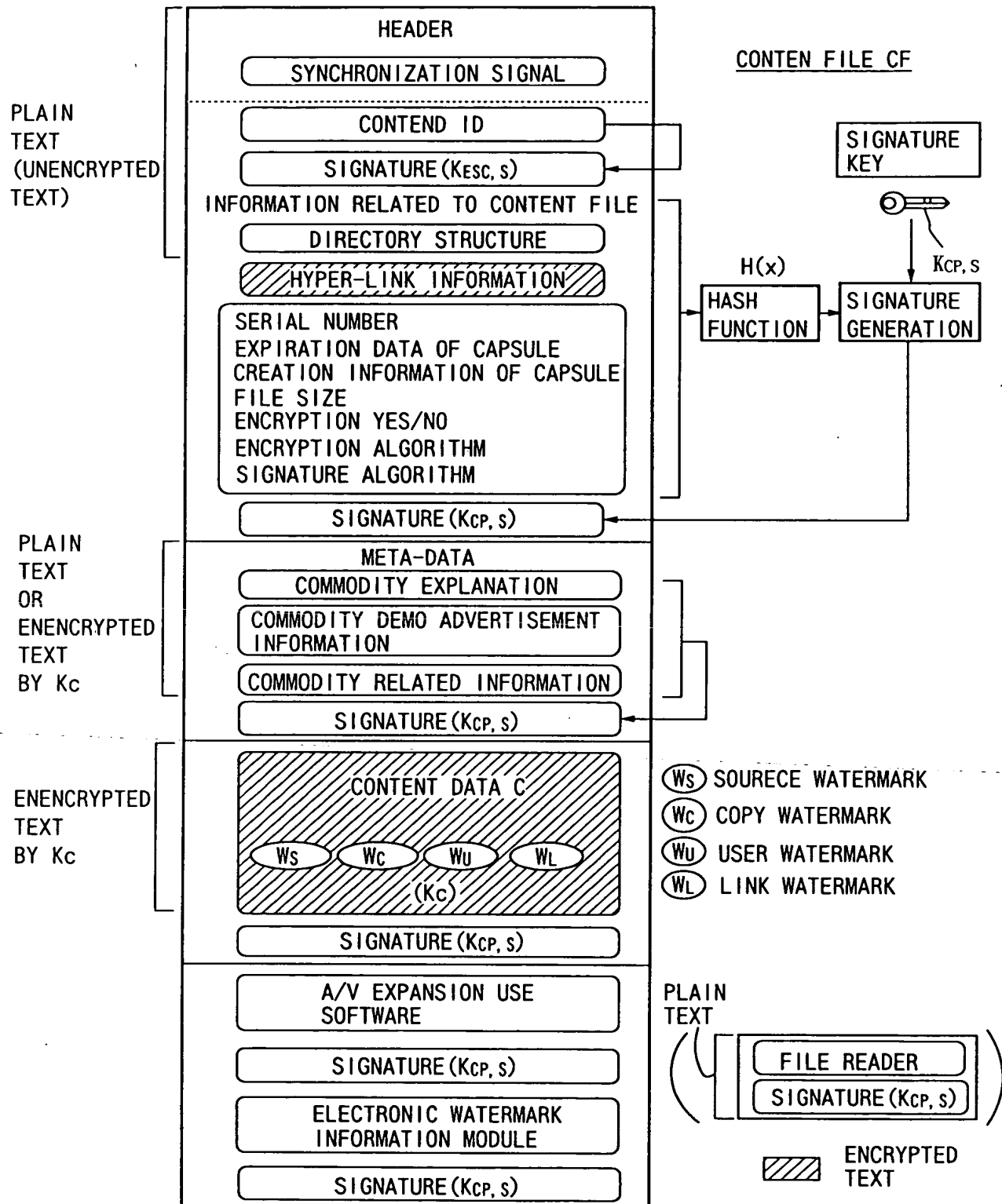


FIG. 5C

FIG.6



KEY FILE CF

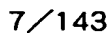


FIG.8

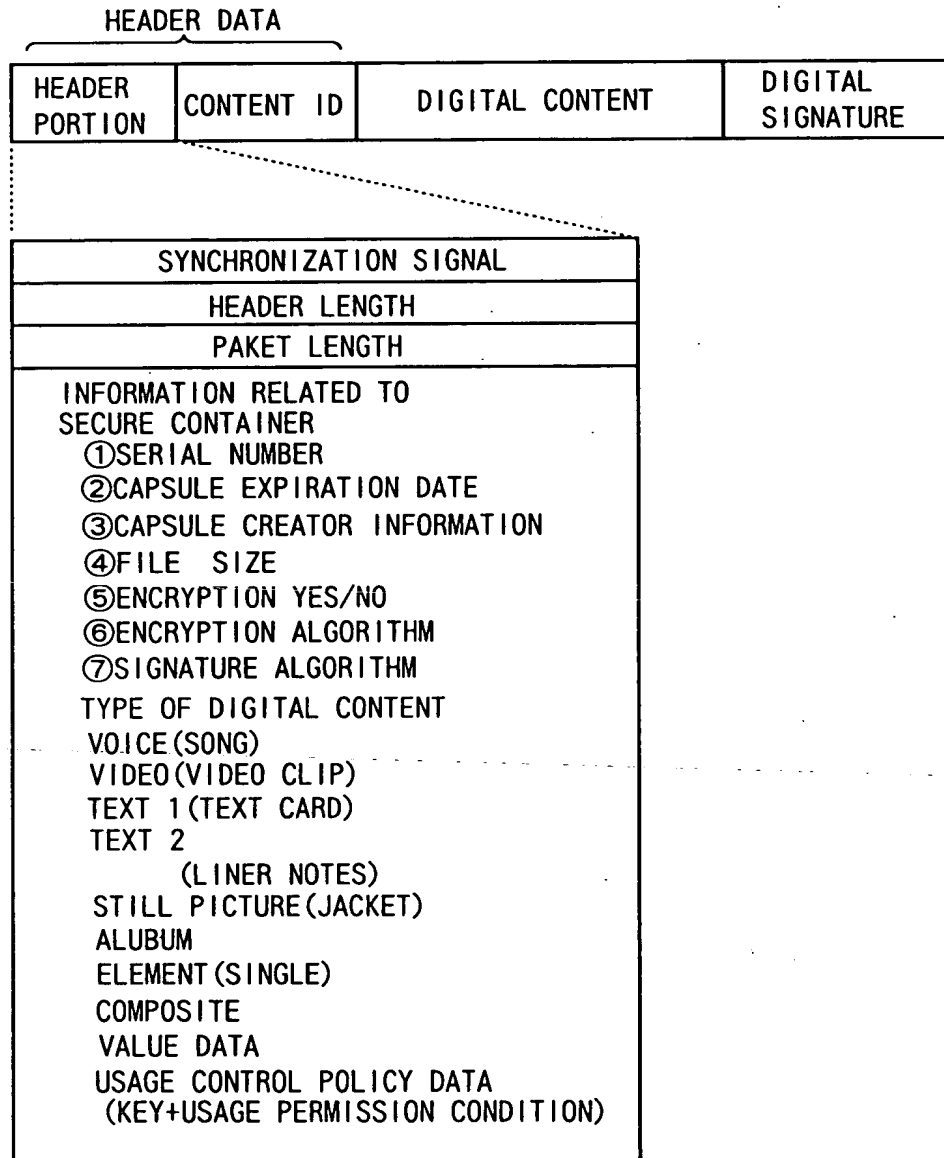


FIG.9

CONTENT ID

FUNDAMENTAL STRUCTURE OF CONTENT ID

ENCIPHERED
TEXT
OR
UNENCIPHERED
TEXT BY
Kc

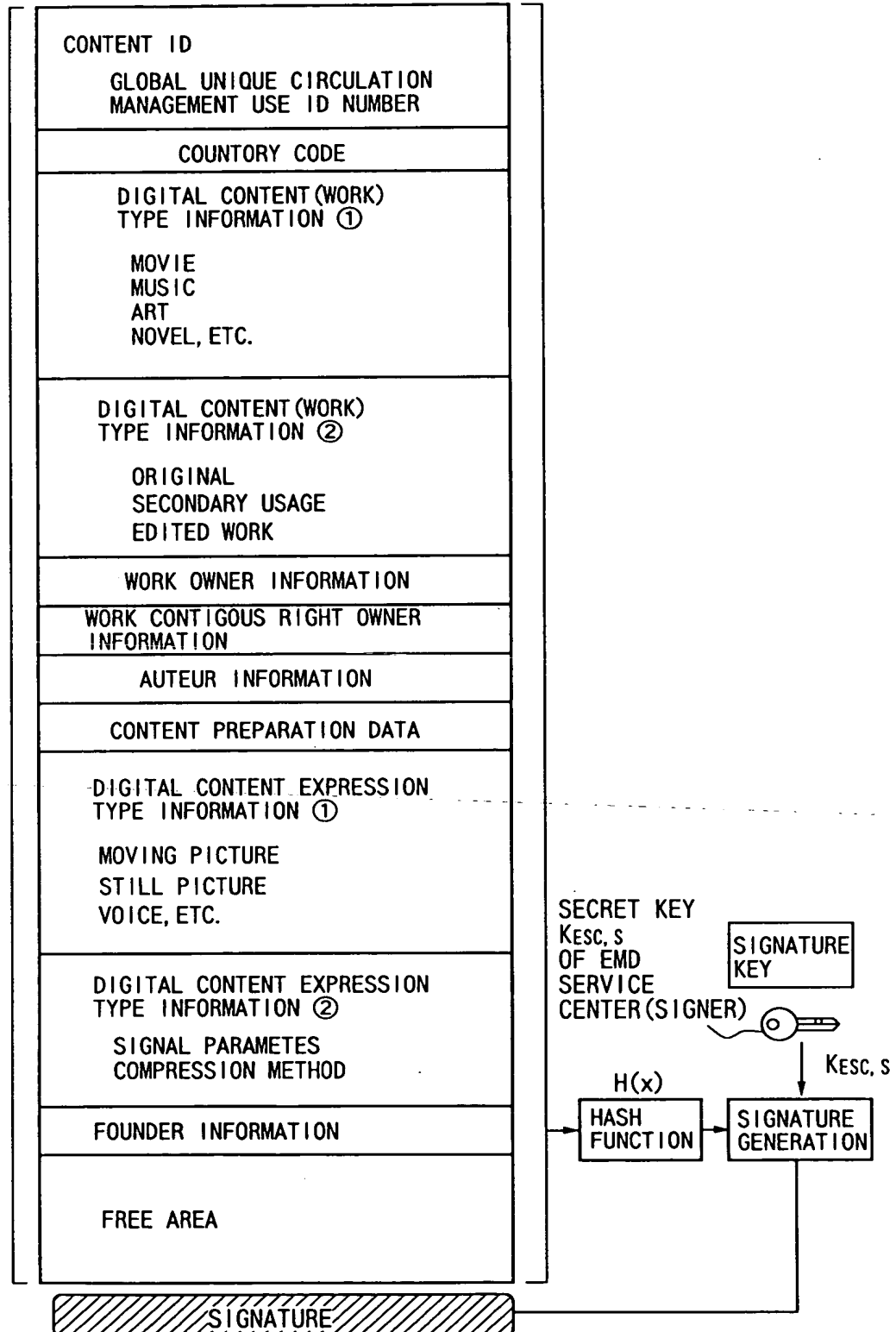


FIG.10

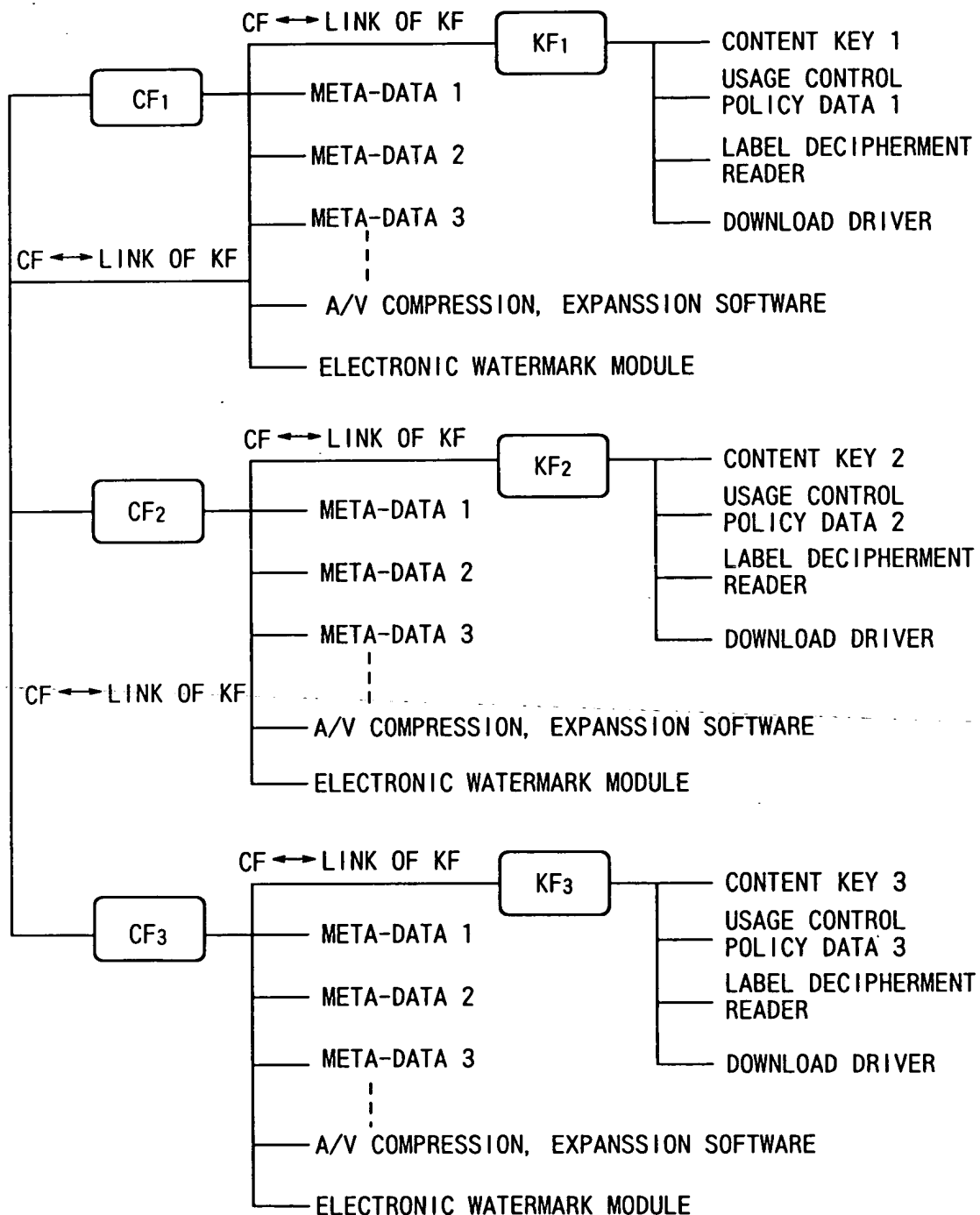
DIRECTORY STRUCTURE OF SECURE CONTAINER

FIG.11
HYPER-LINK DATA OF SECURE CONTAINER

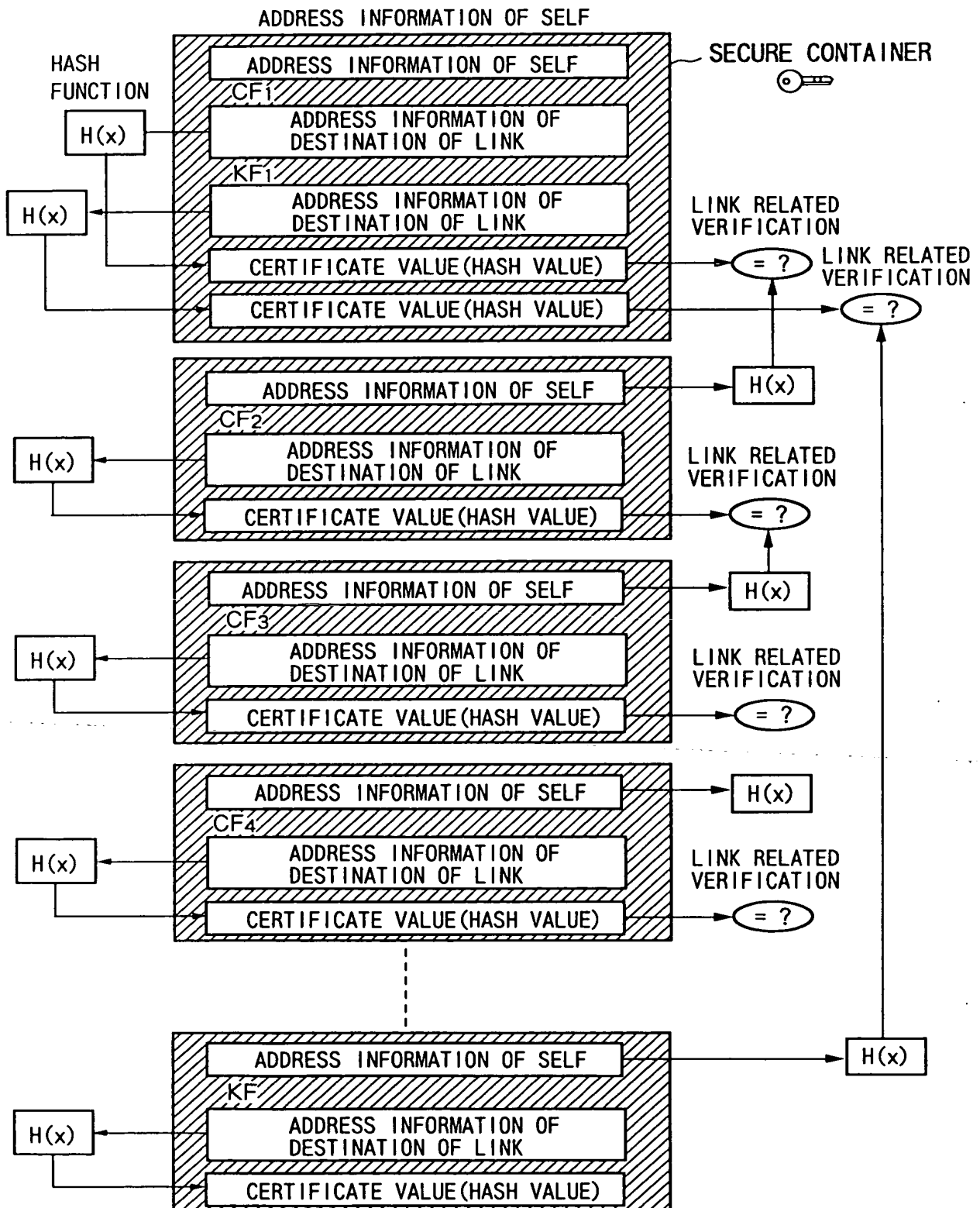


FIG.12

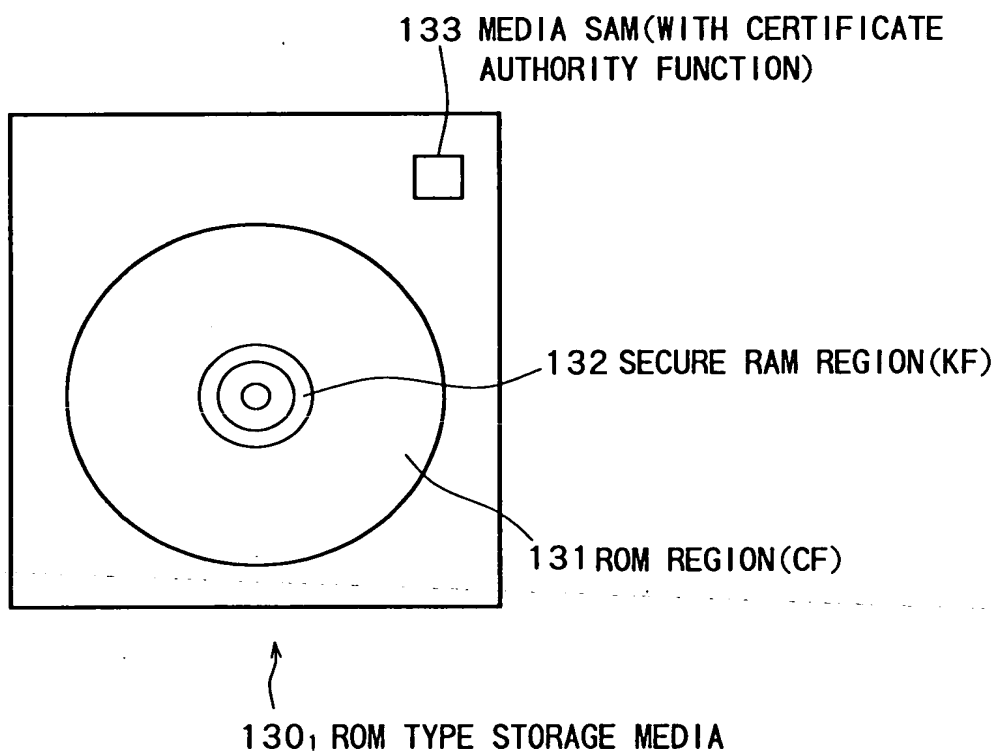


FIG.13

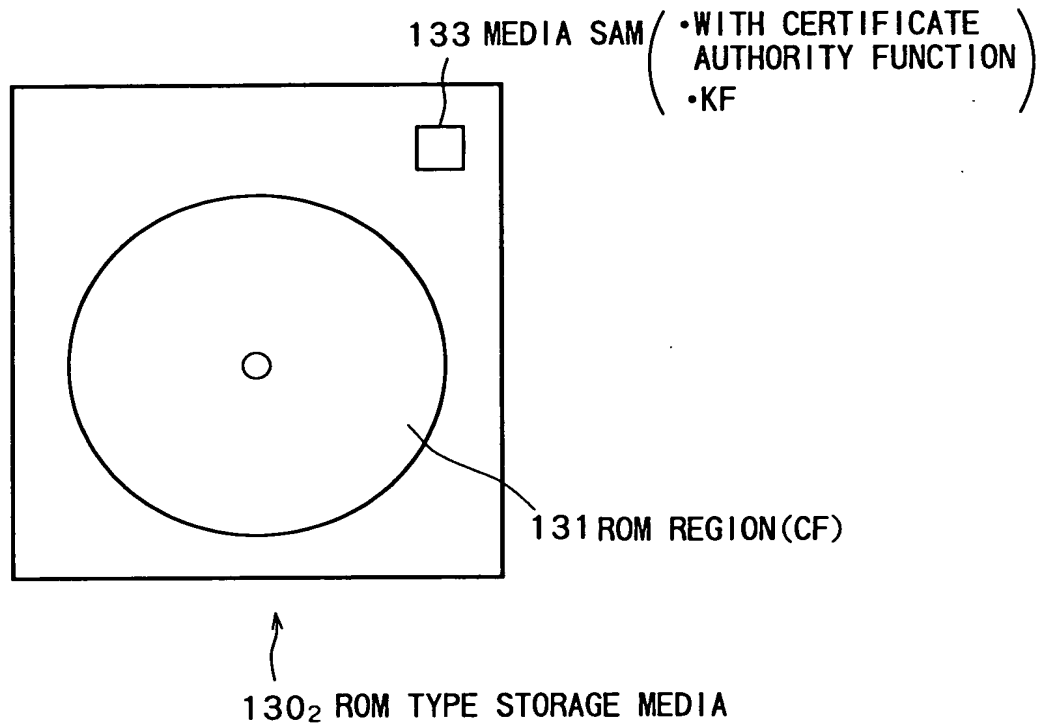


FIG.14

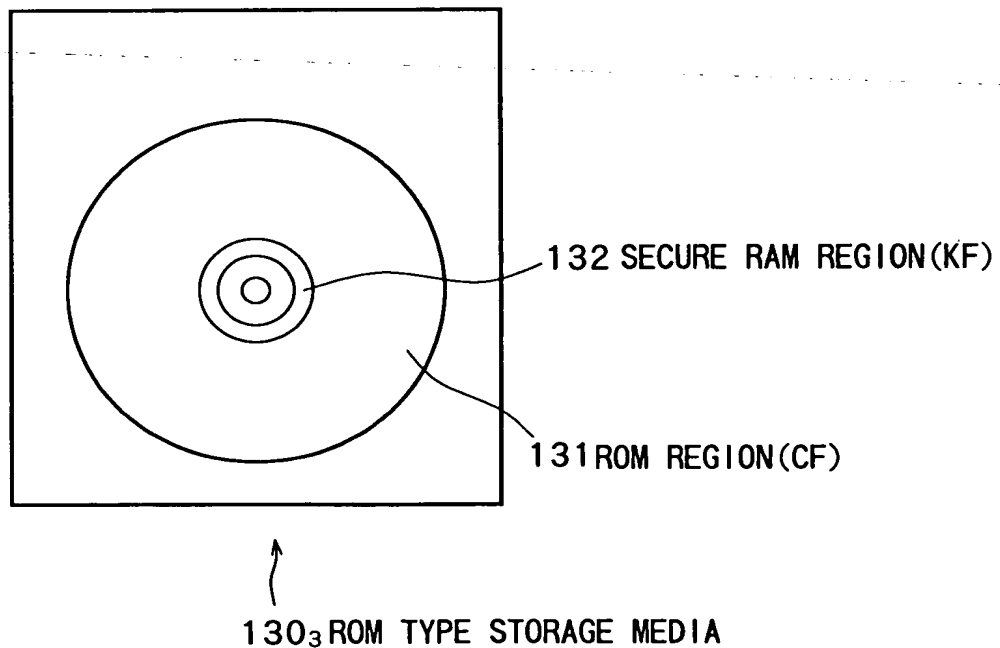


FIG.15

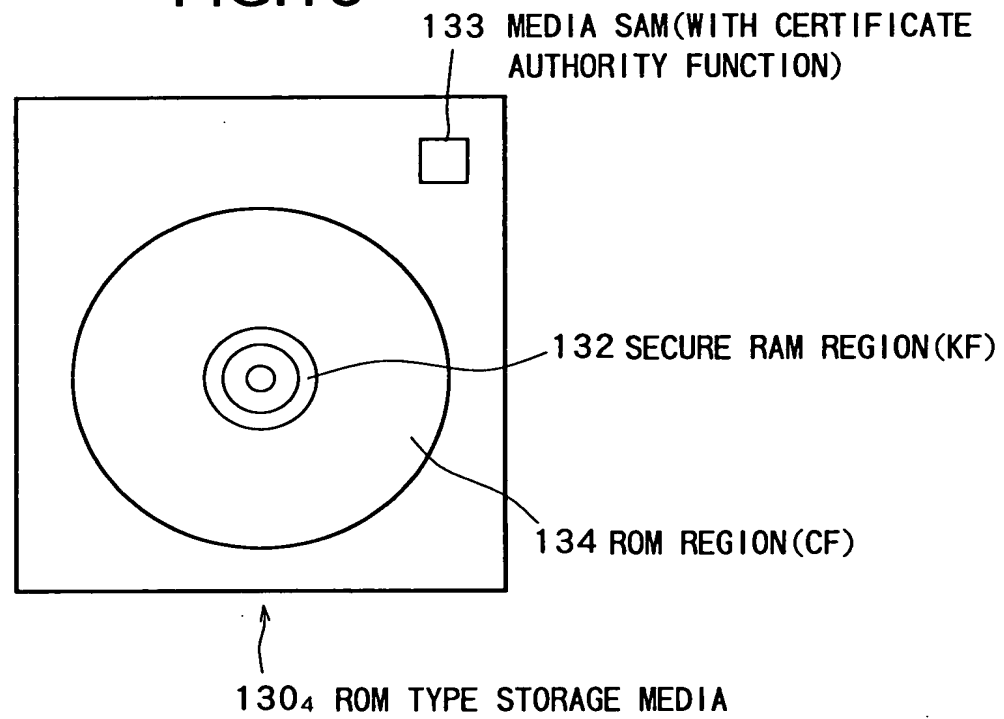


FIG.16

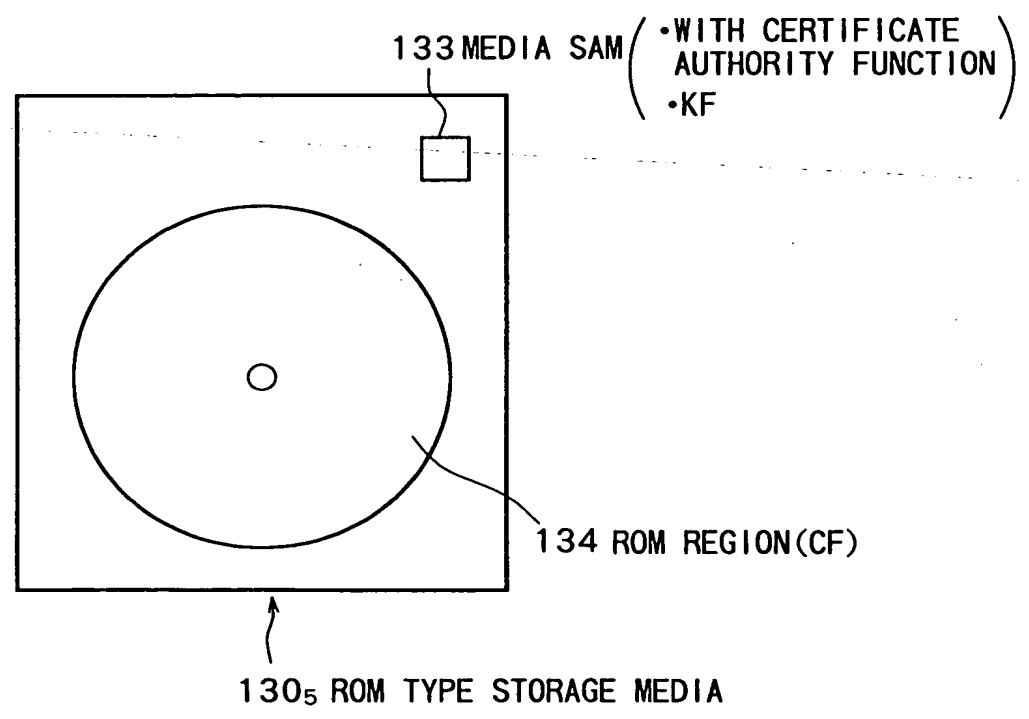
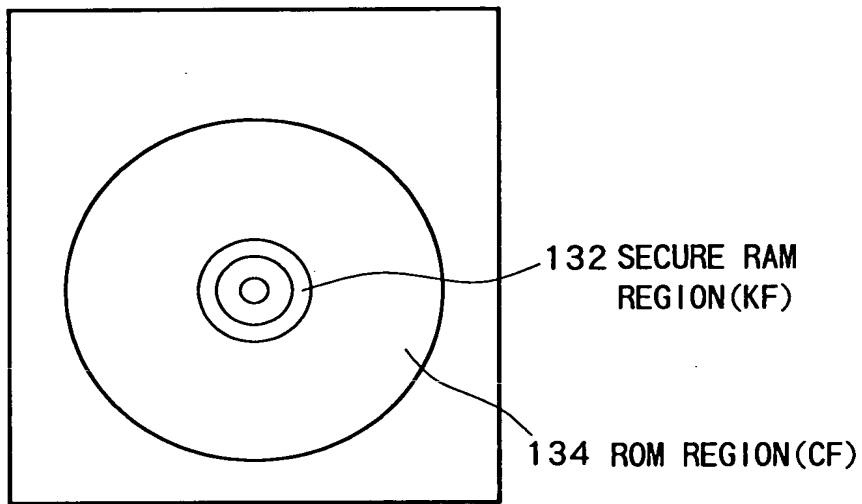


FIG.17



130₆ ROM TYPE STORAGE MEDIA

FIG. 18

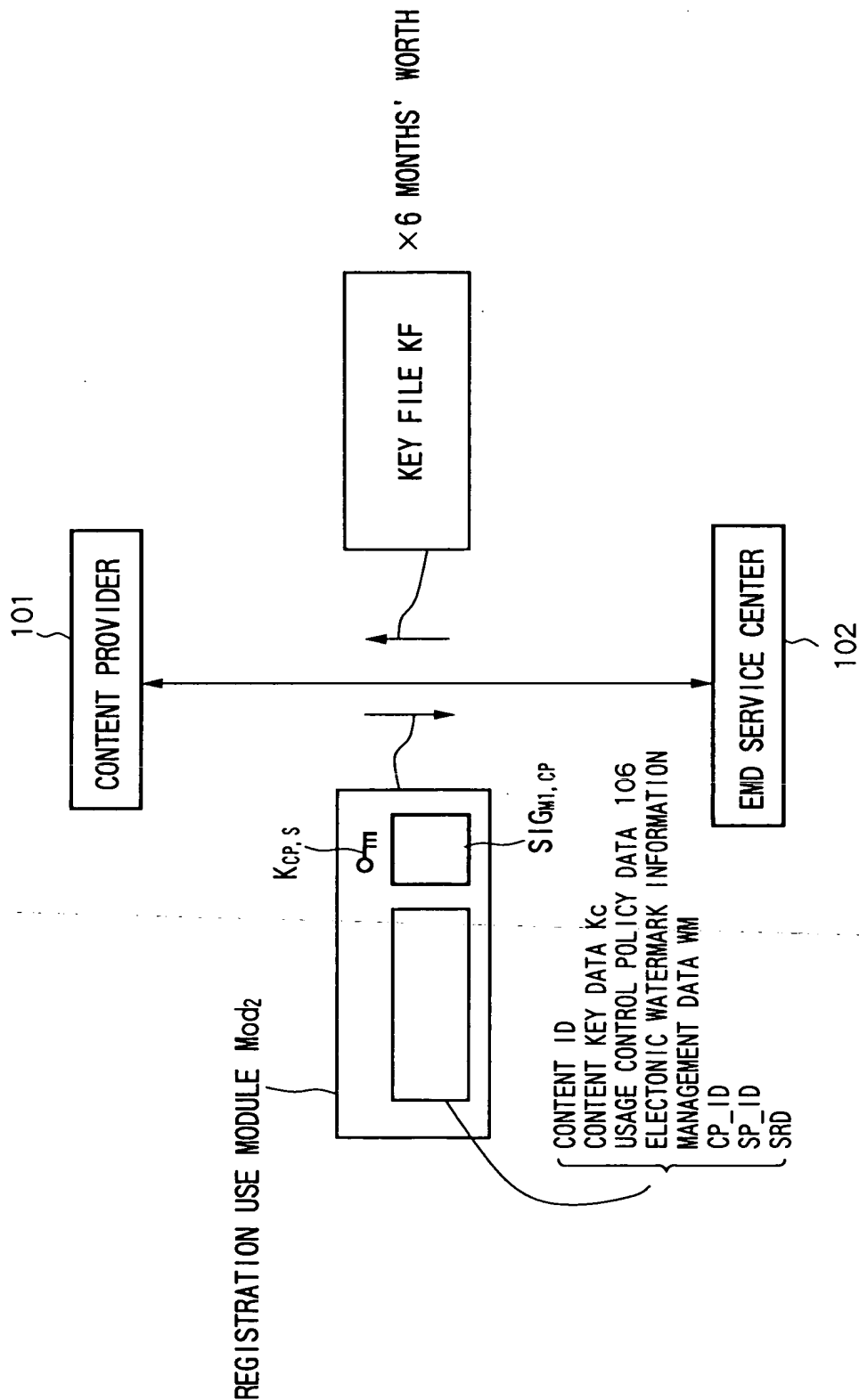


FIG.19

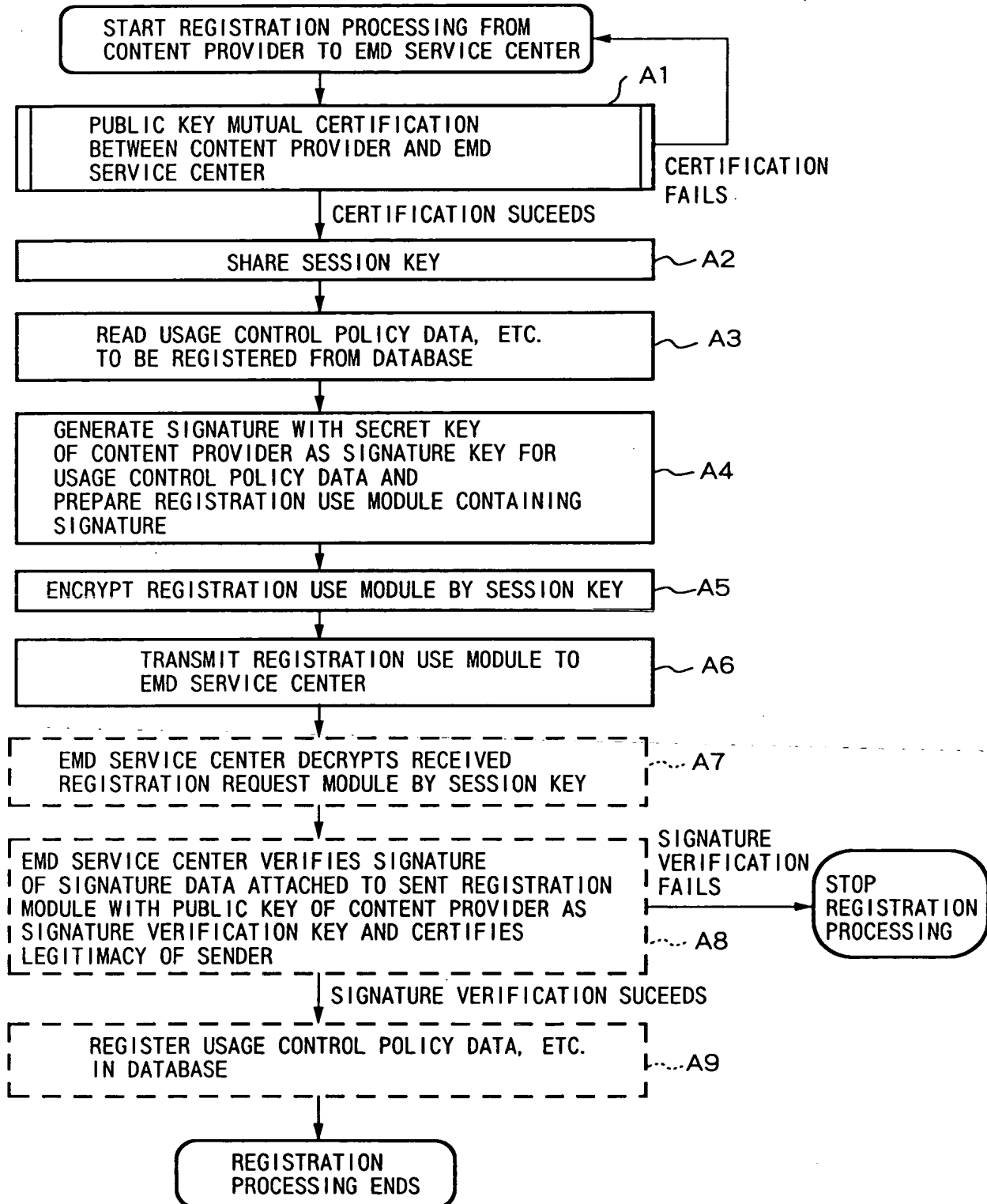


FIG. 20

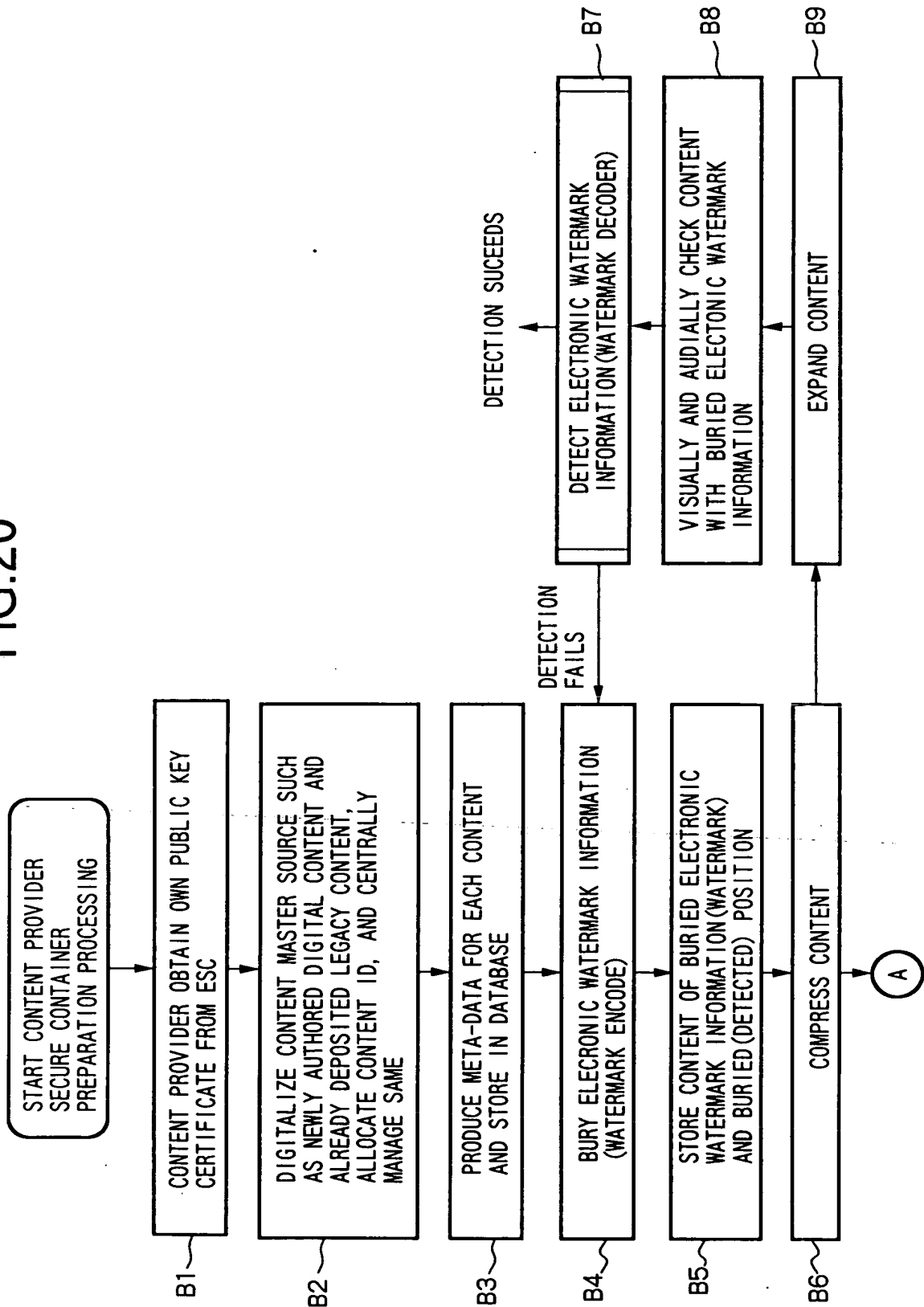


FIG.21

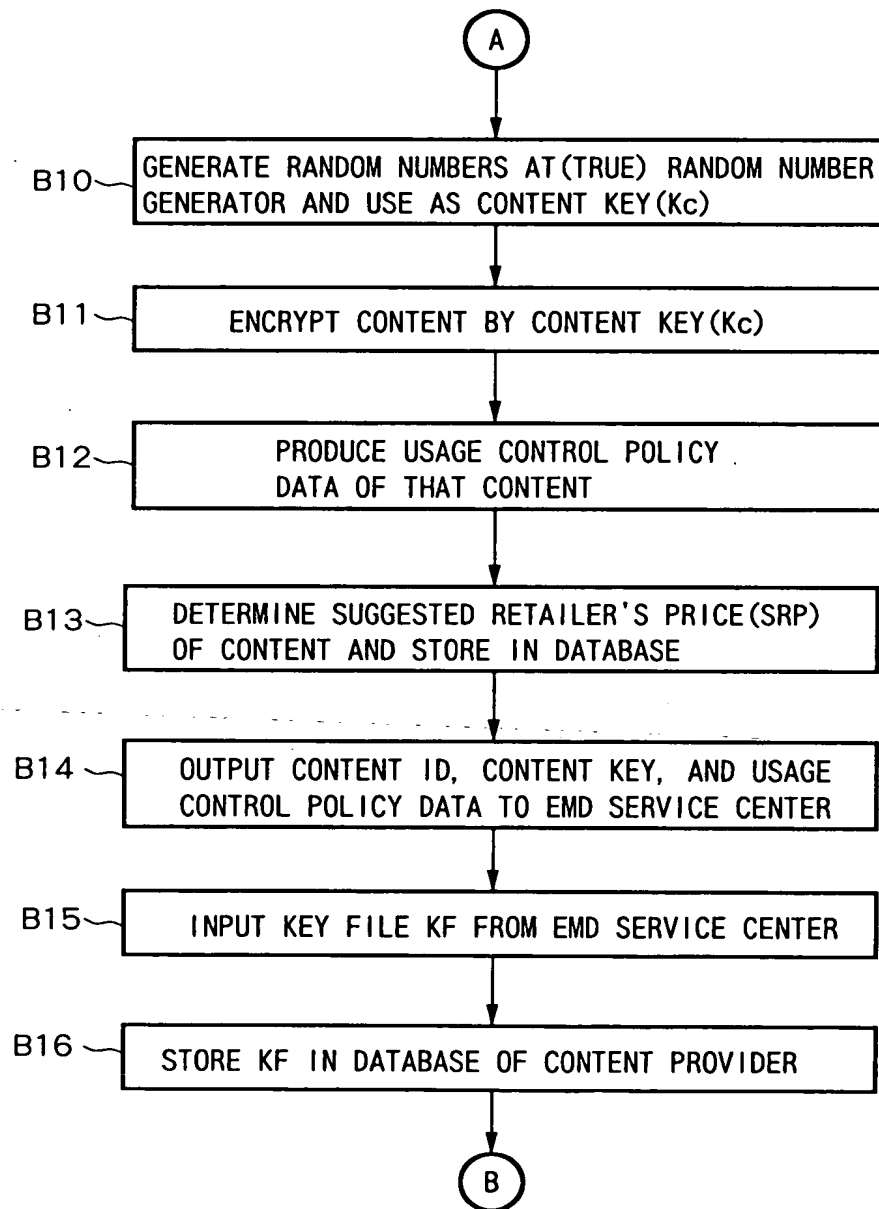


FIG.22

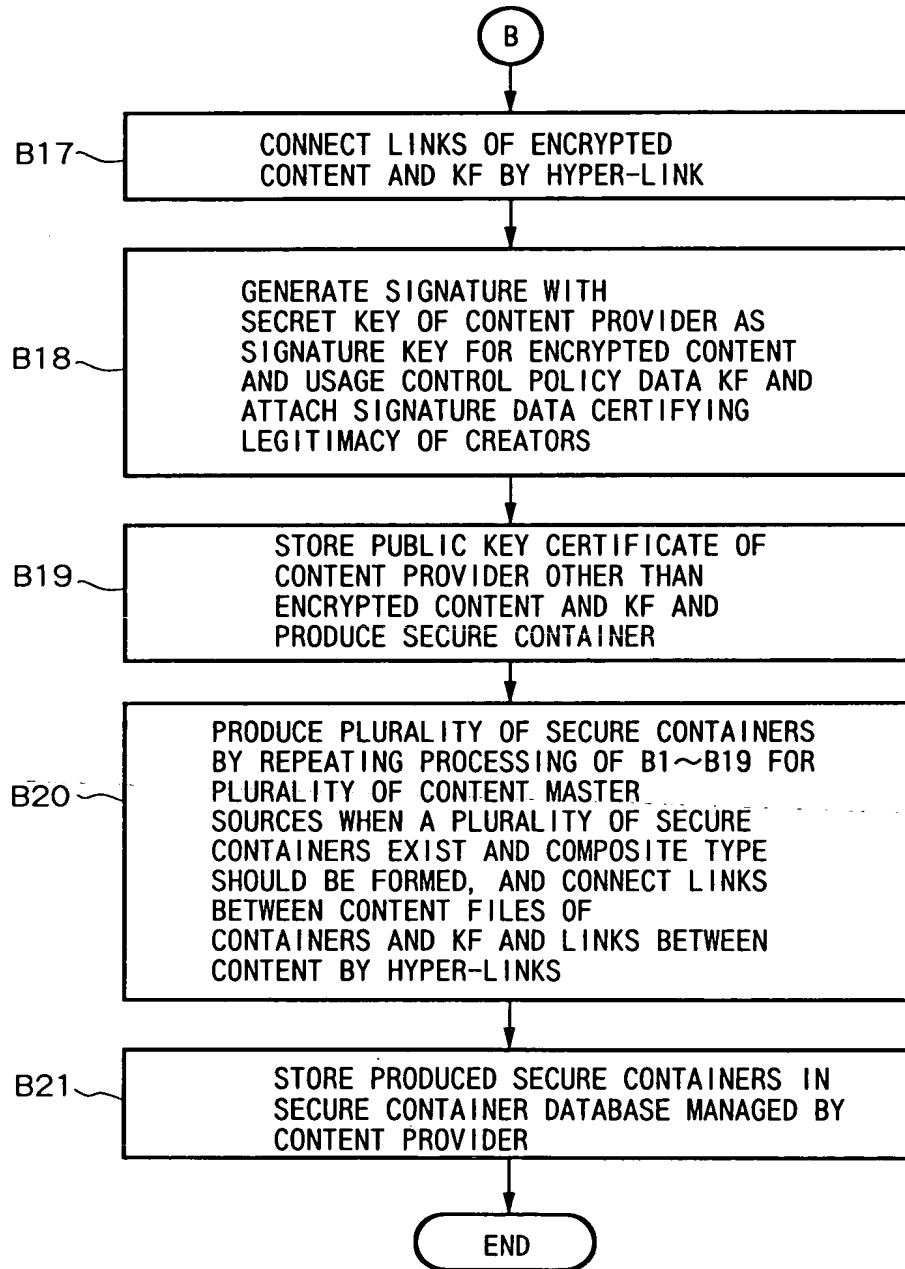
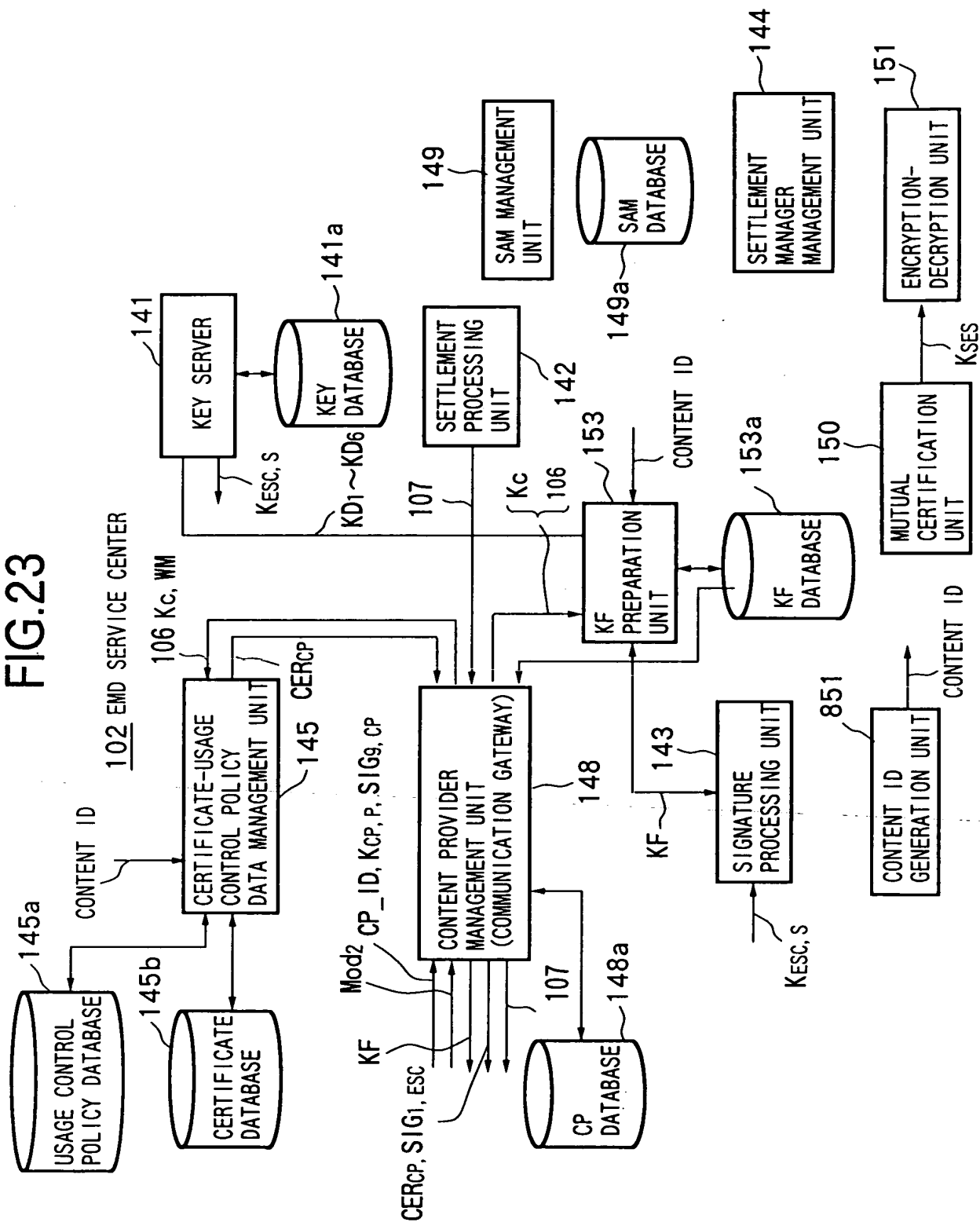


FIG. 23



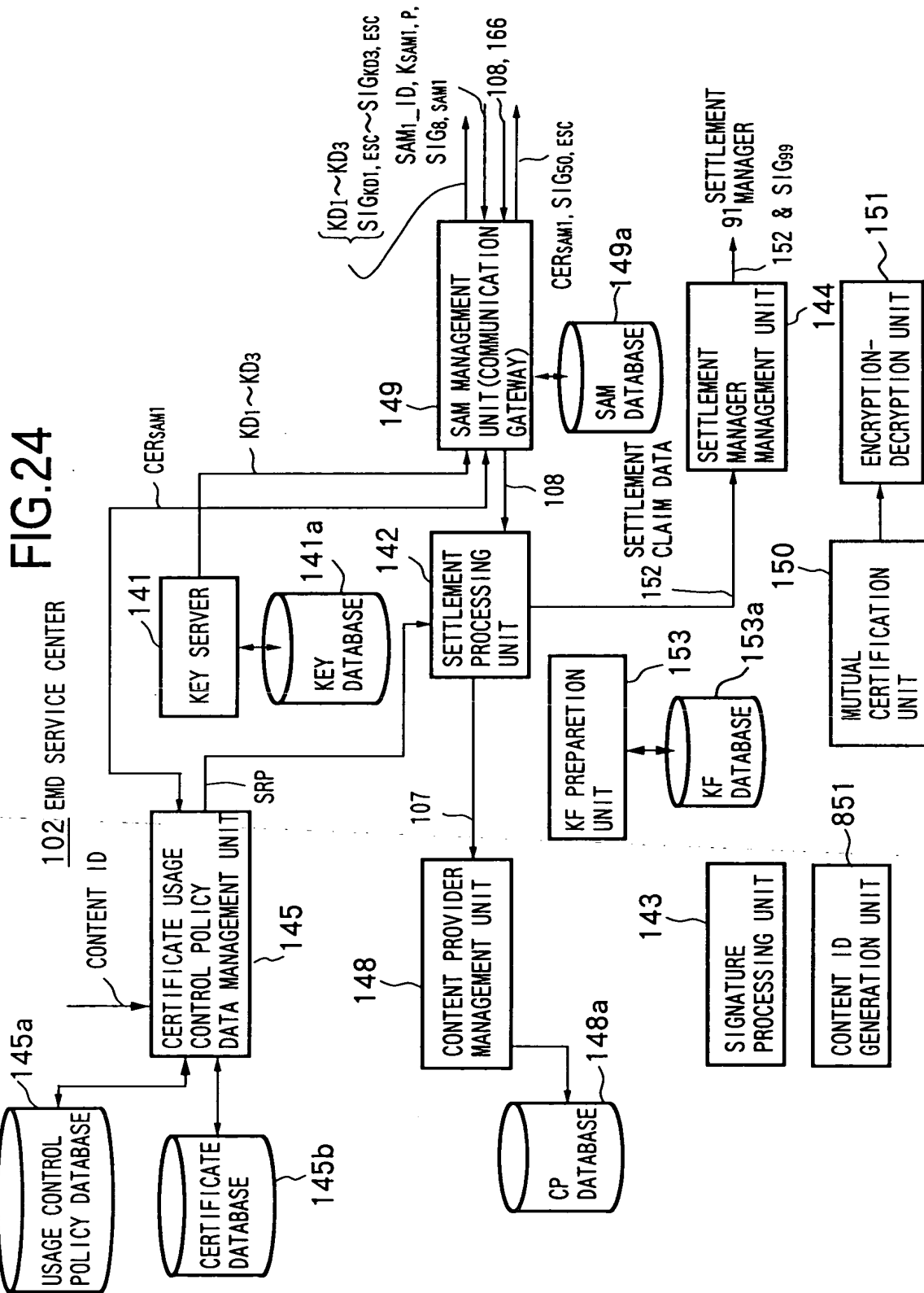
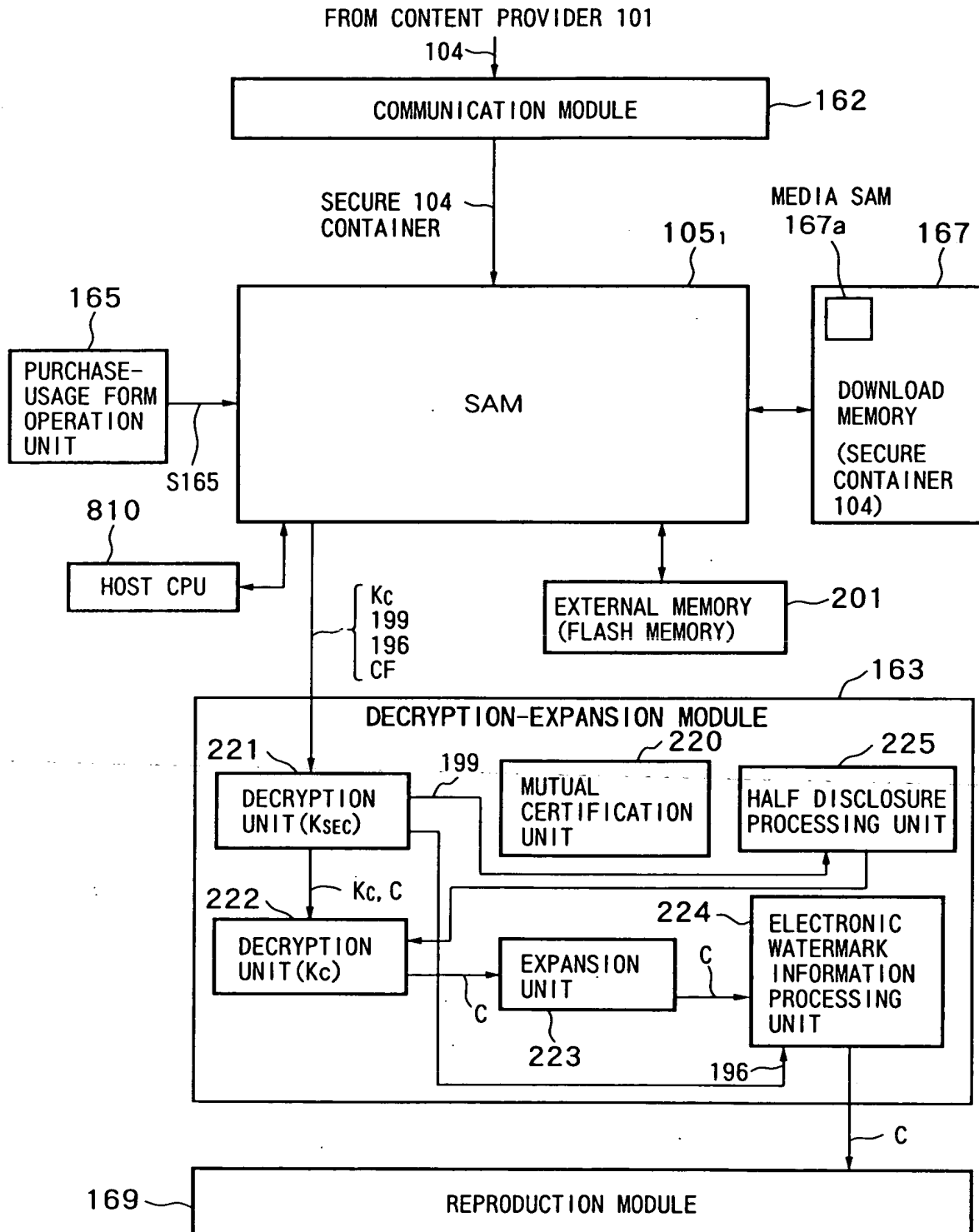


FIG.25



SAM 1051

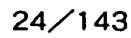


FIG.27

DATA STORED IN EXTERNAL MEMORY 201

USAGE LOG DATA 108
SAM REGISTRATION LIST

FIG.28

DATA STORED IN STACK MEMORY 200

CONTENT KEY DATA K_c
USAGE CONTROL POLICY DATA(USP) 106
LOCK KEY DATA K_{Log} OF STORAGE UNIT(FLASH MEMORY) 192
CERTIFICATE CER_{CP} OF CONTENT PROVIDER 101
USAGE CONTROL STATUS DATA(UCS) 166
SAM PROGRAM DOWNLOADER CONTAINERS SD_1 TO SD_3

FIG.29

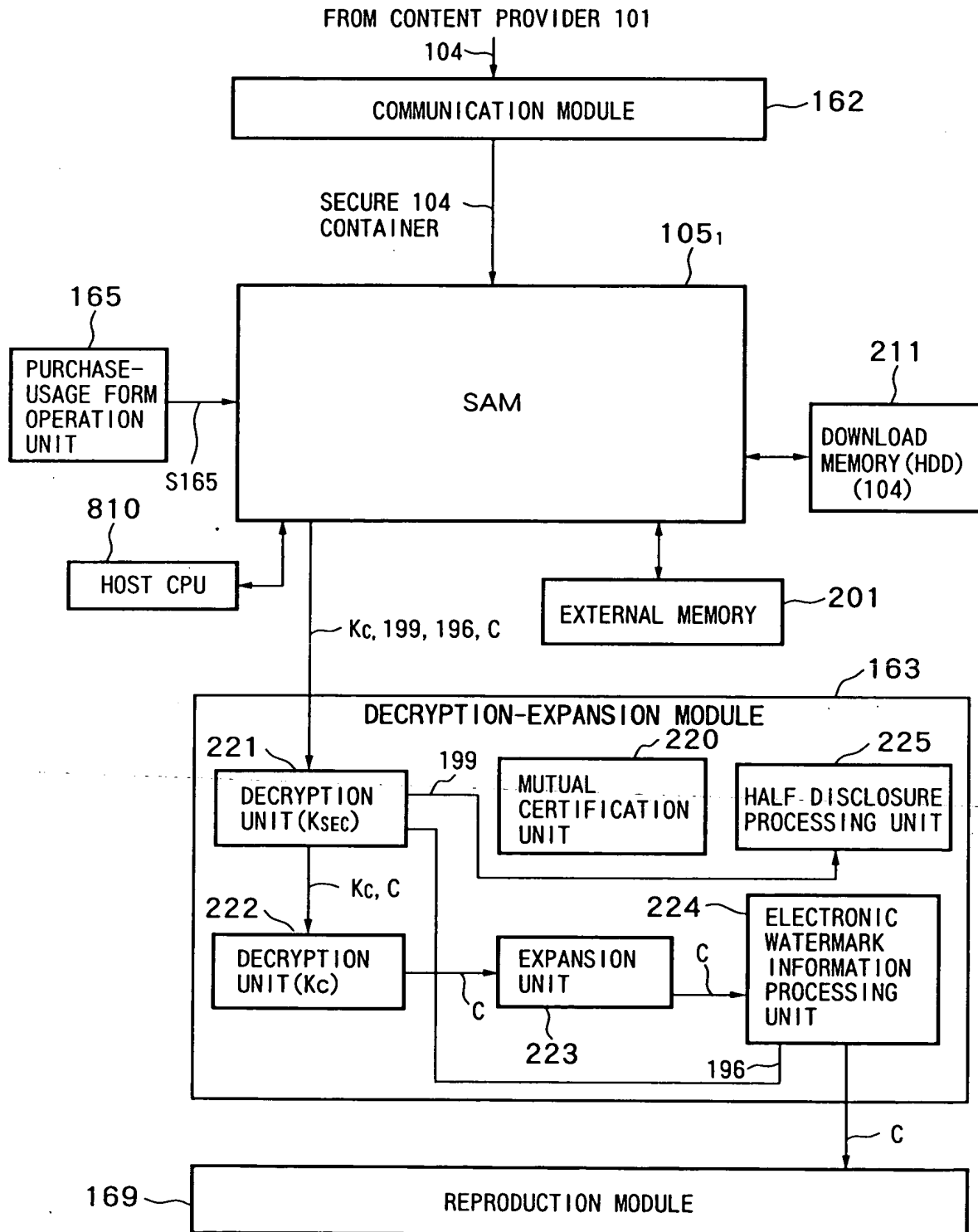
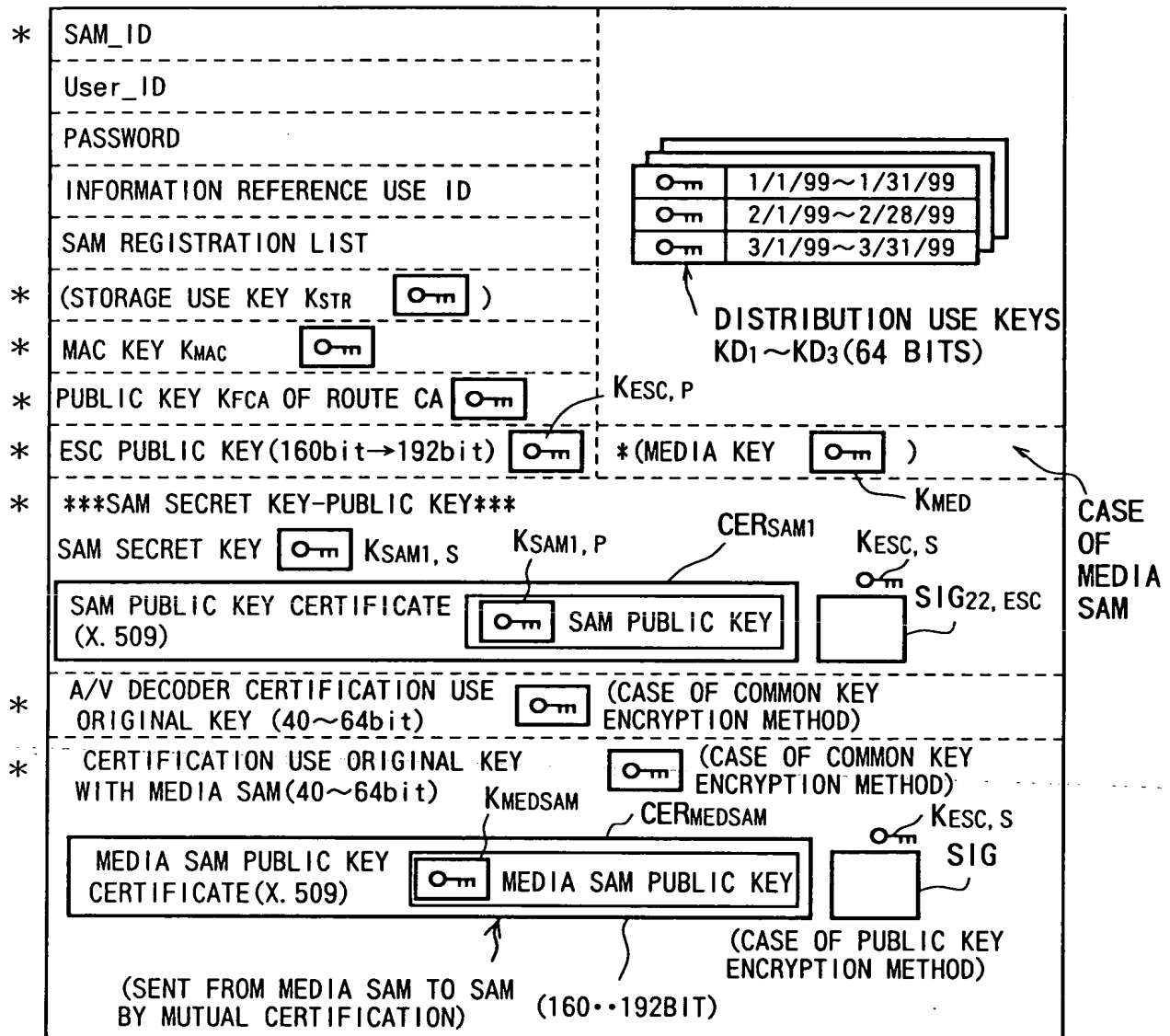


FIG.30

DATA STORED IN STORAGE UNIT 192



1051~1054 SAM



SECURE

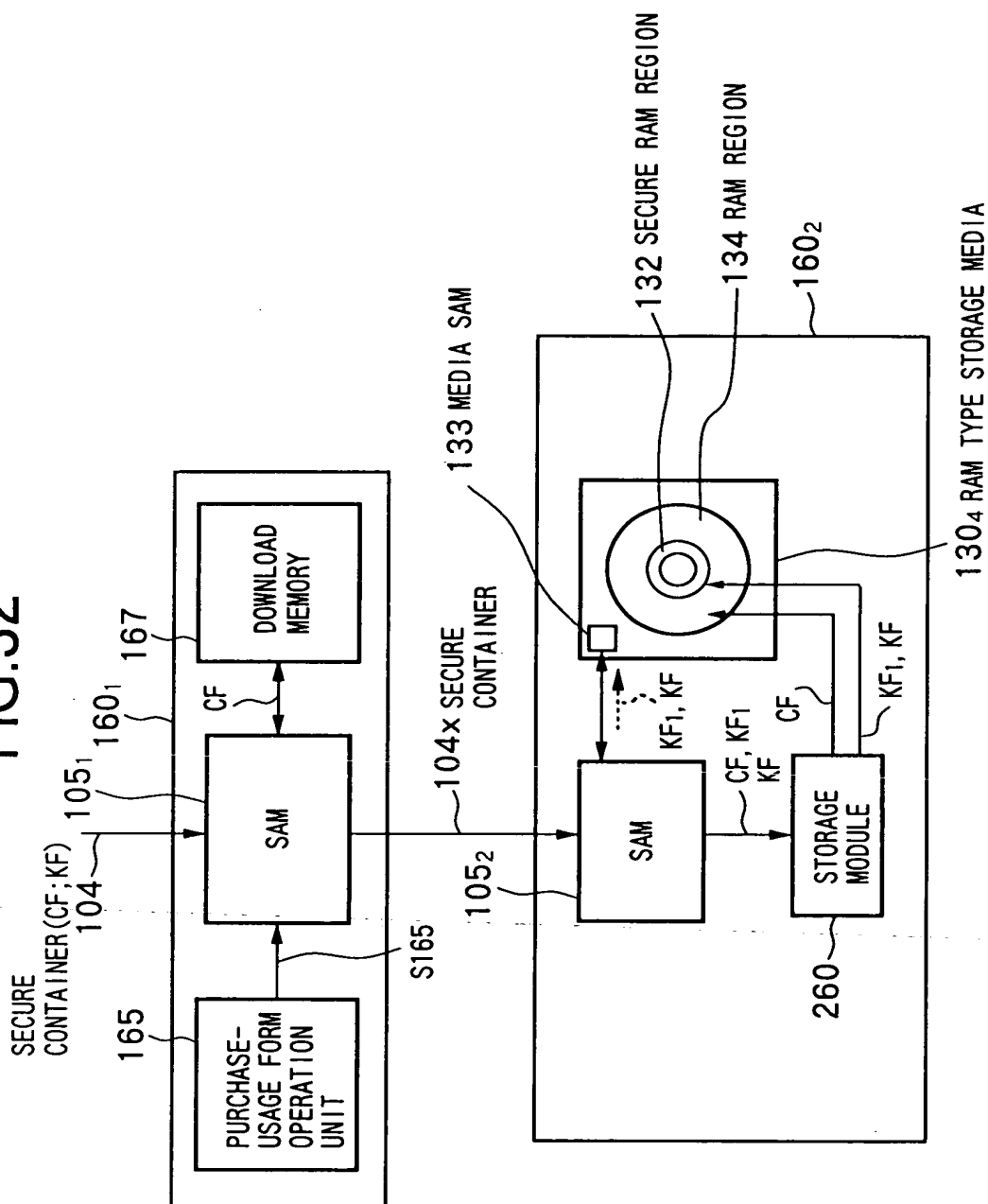
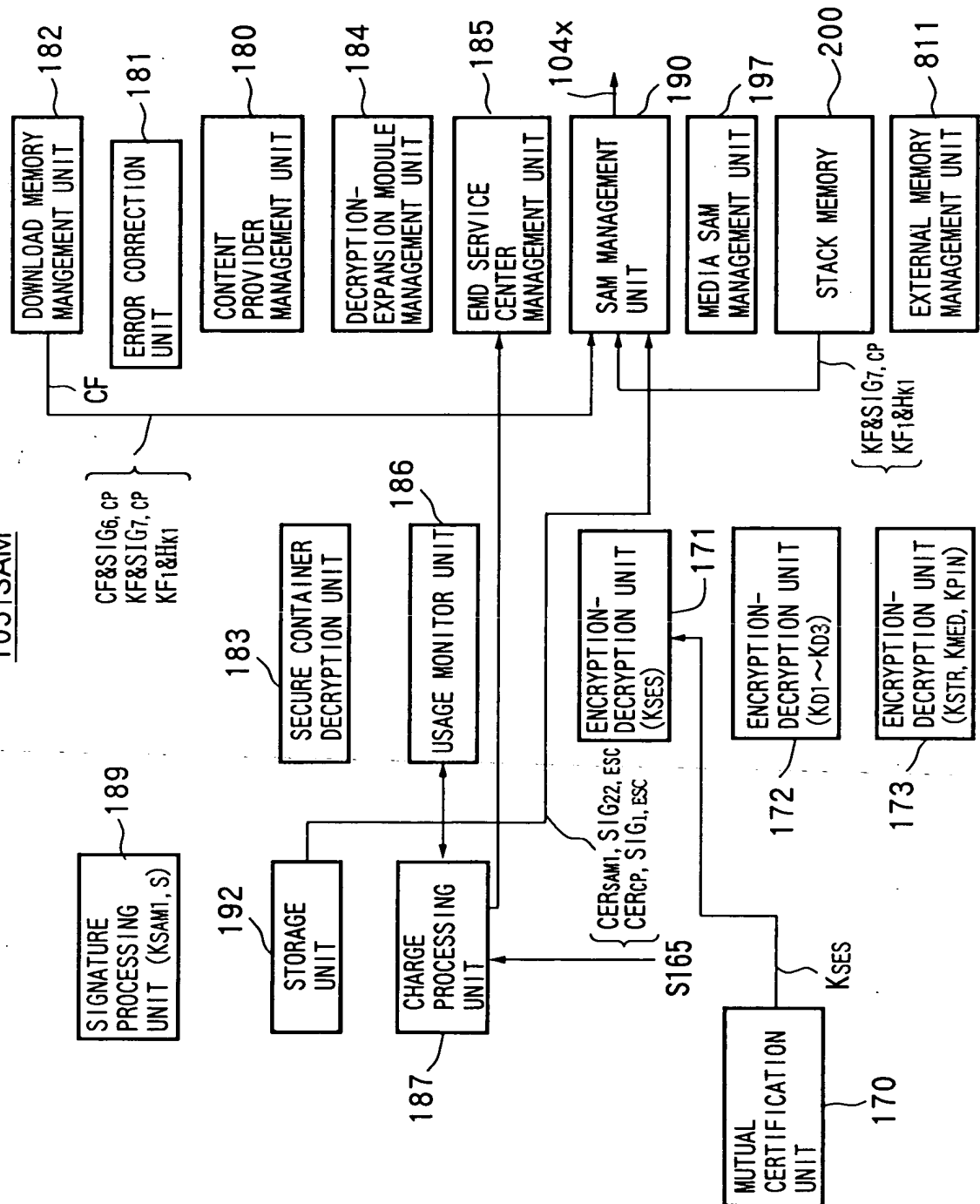


FIG. 33

1051SAM



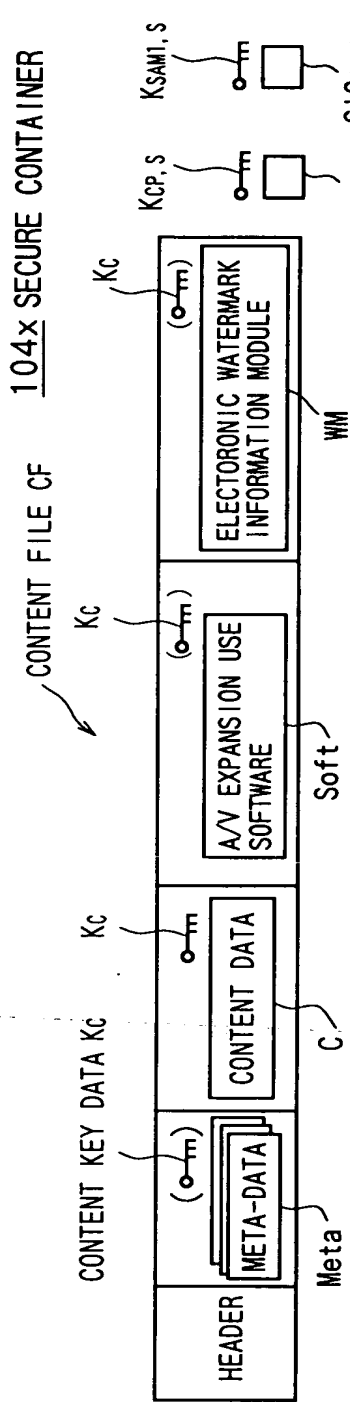


FIG. 34A

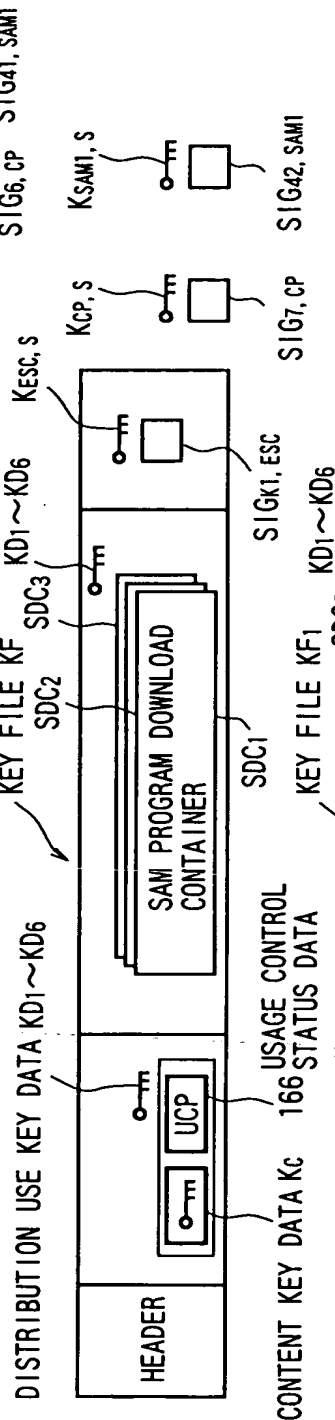


FIG. 34B

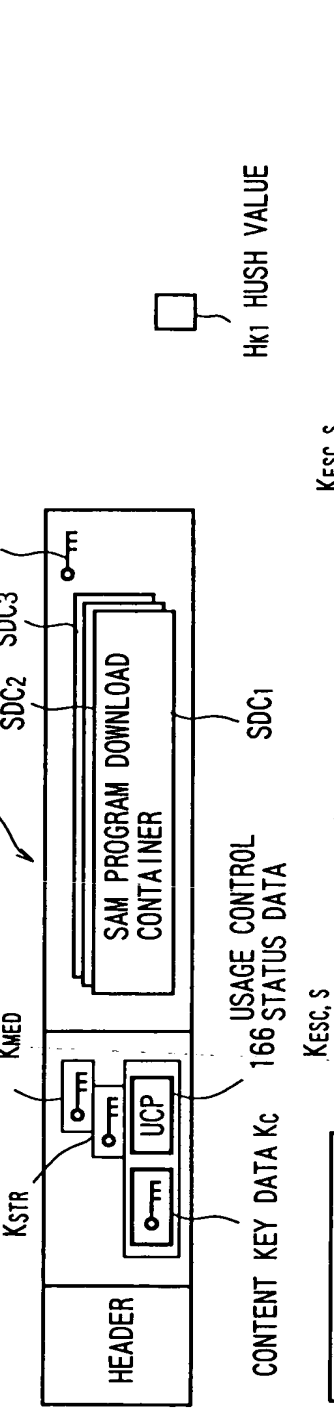


FIG. 34C

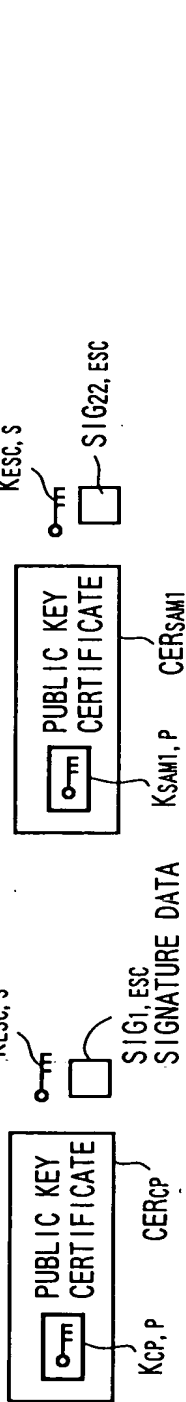


FIG. 34D

FIG. 35

SAM1052

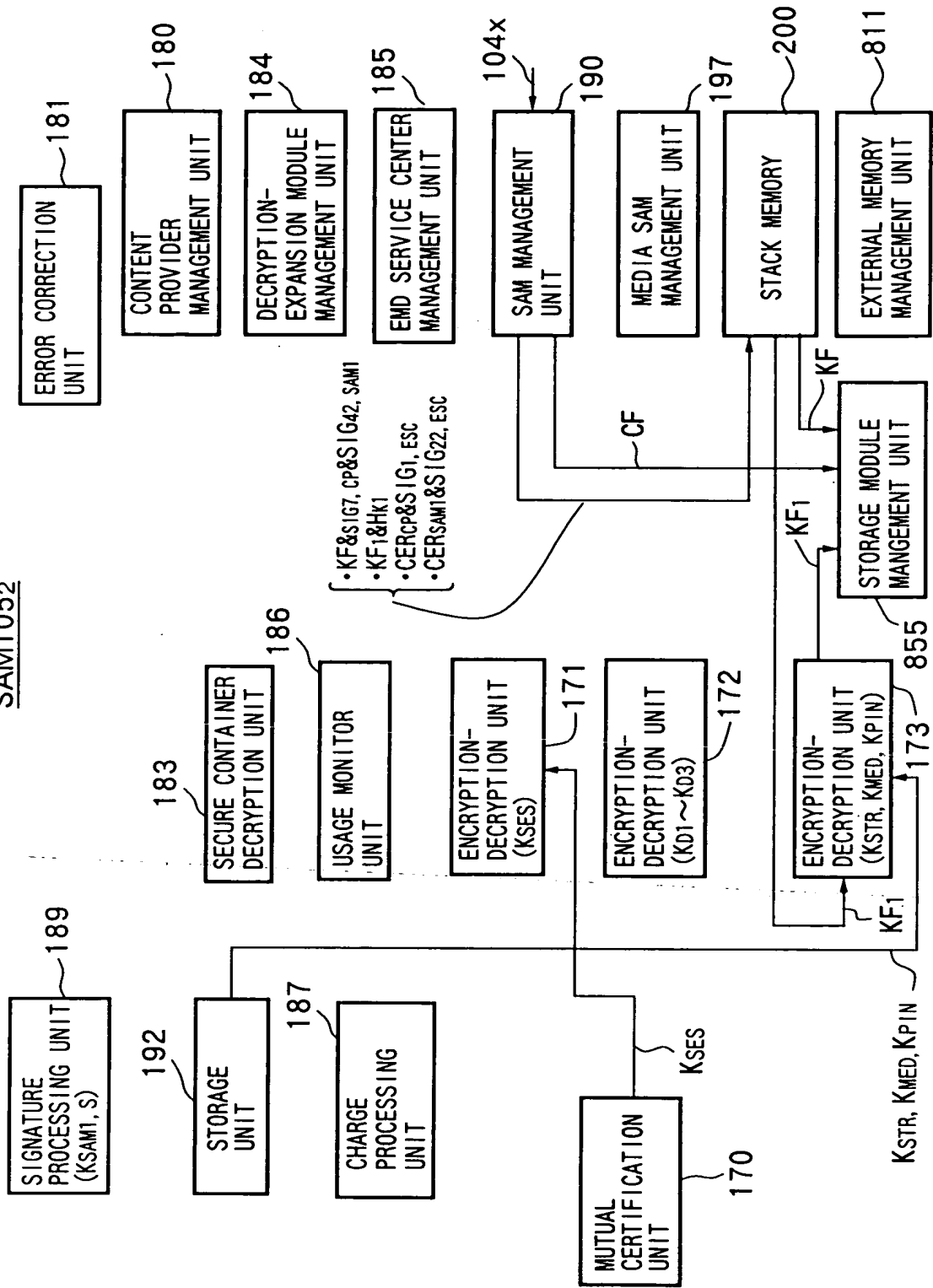


FIG. 36

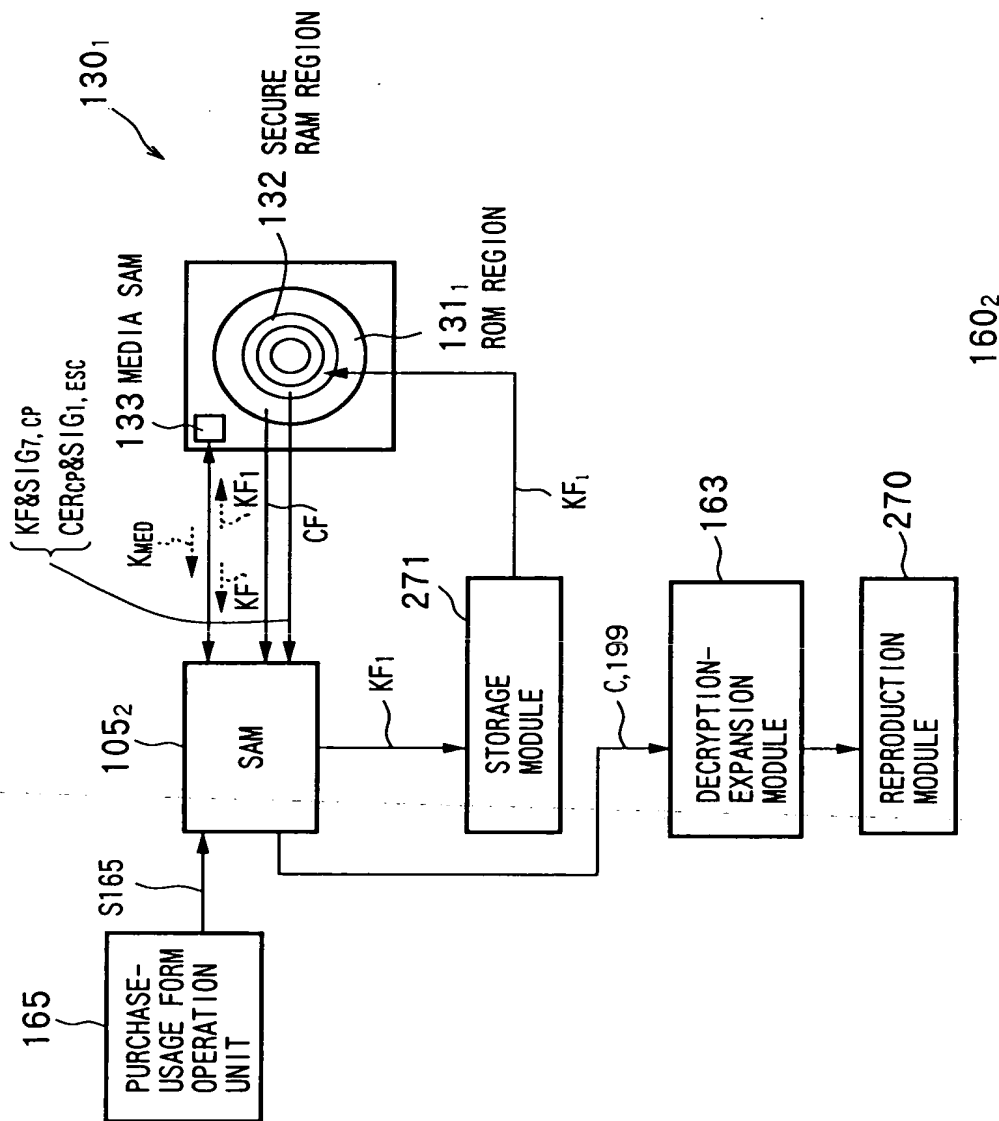


FIG.38

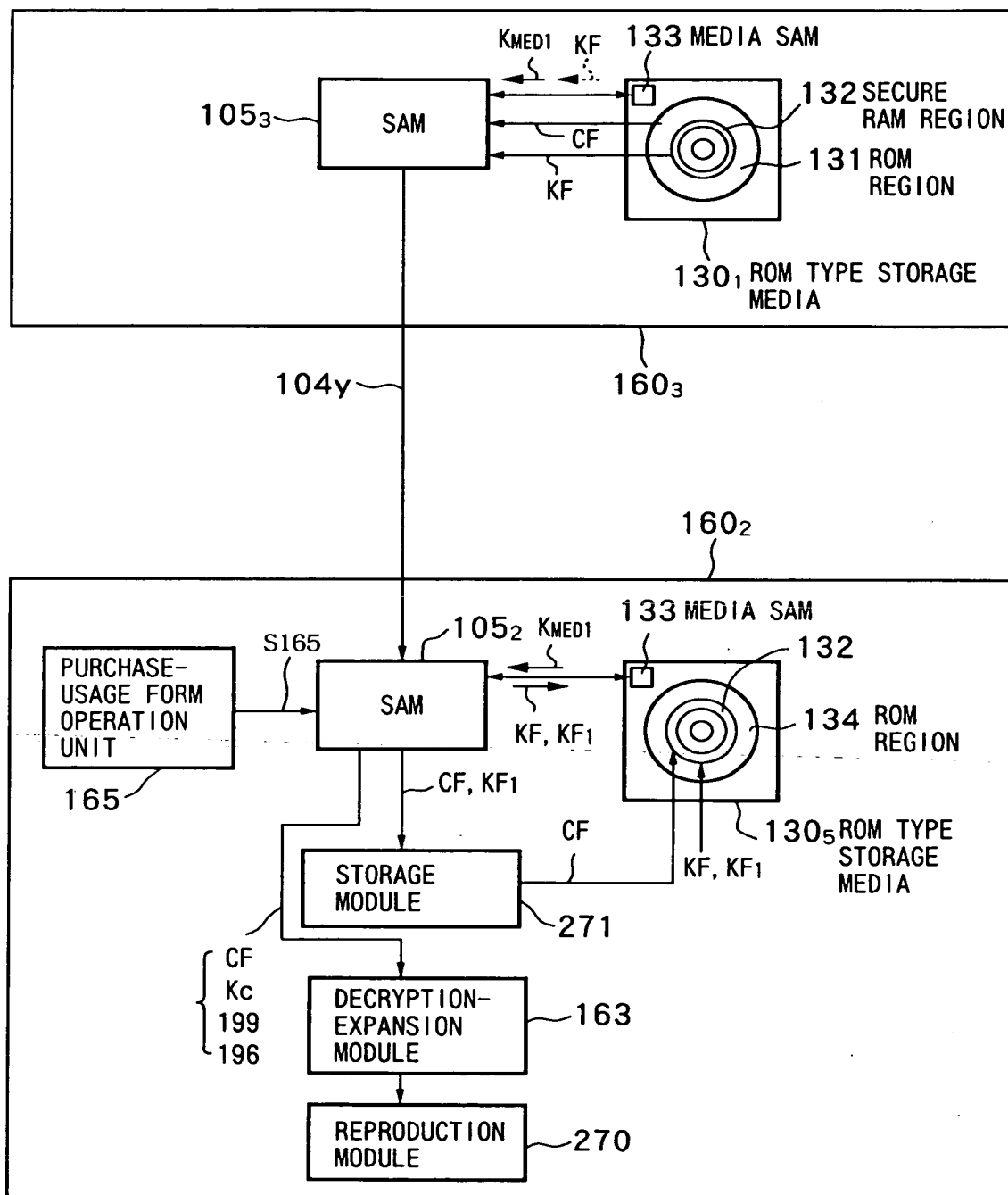
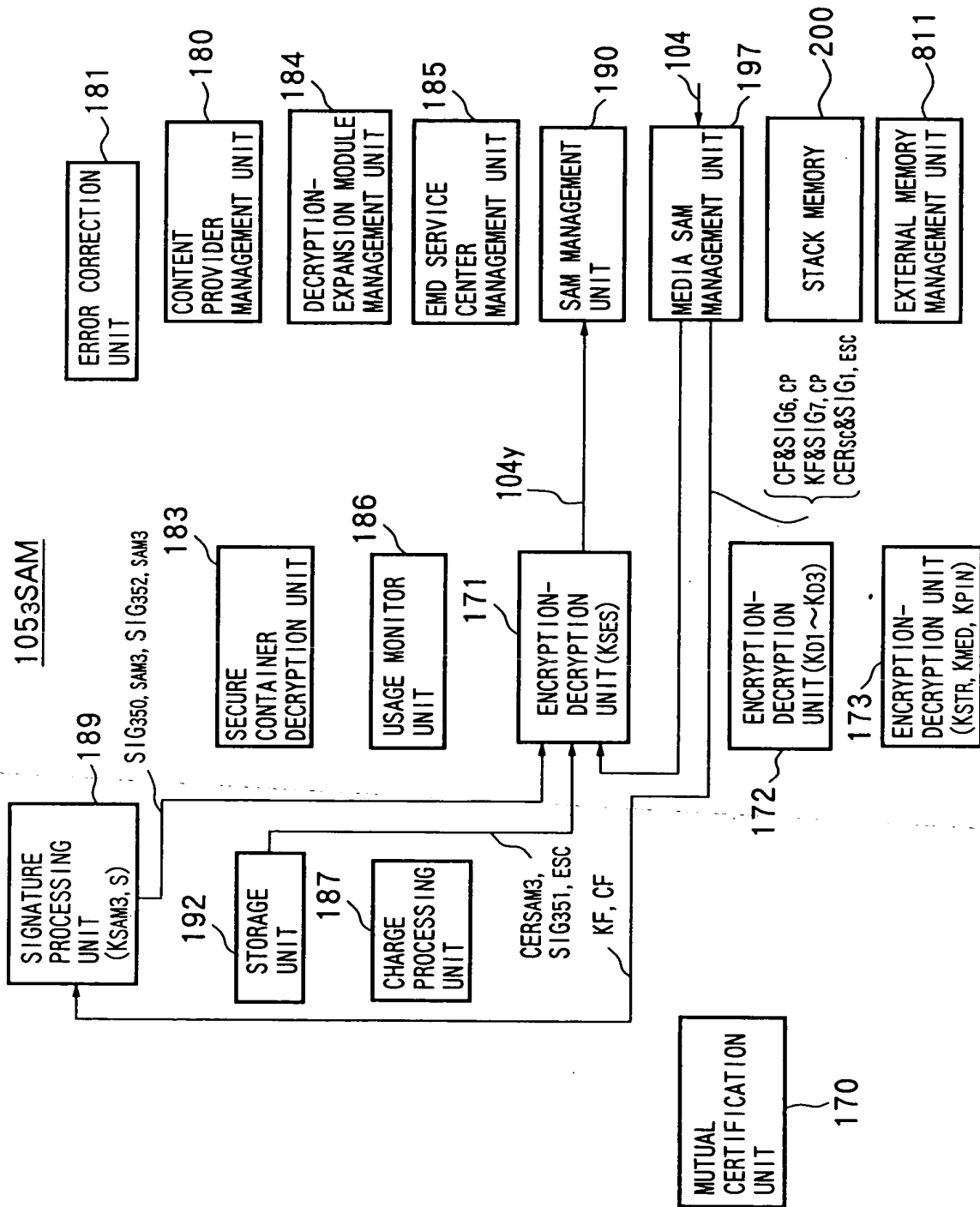


FIG. 39



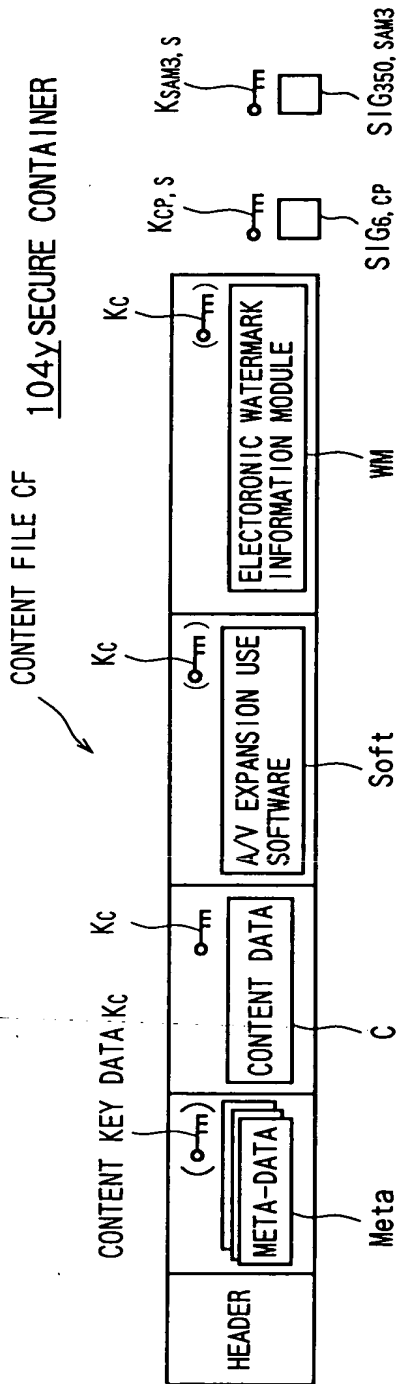


FIG. 40A

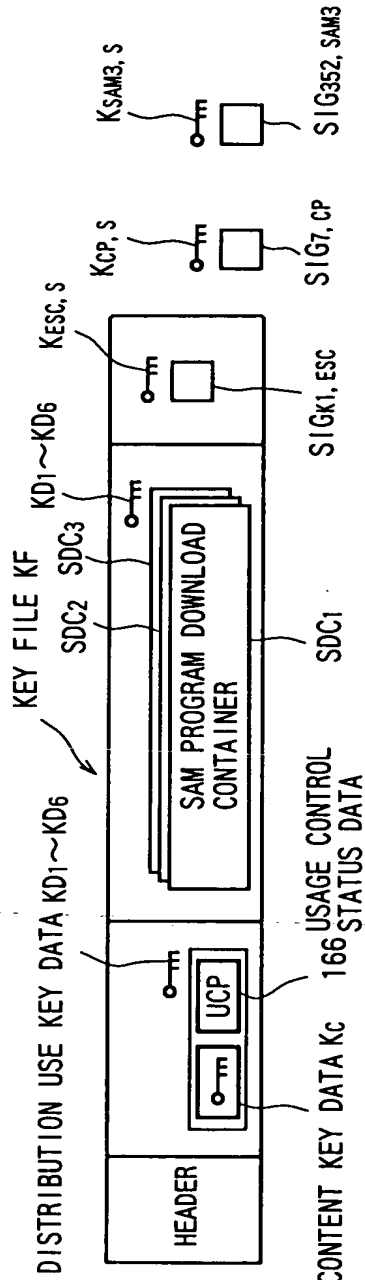


FIG. 40B

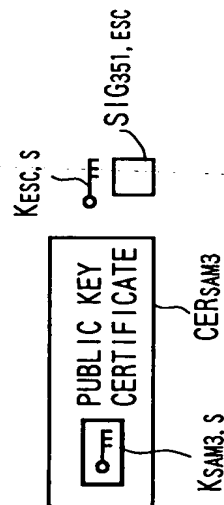


FIG. 40C

[illegible]

FIG.42A 101 (CP) → SAM105₁
(IN-BAND)

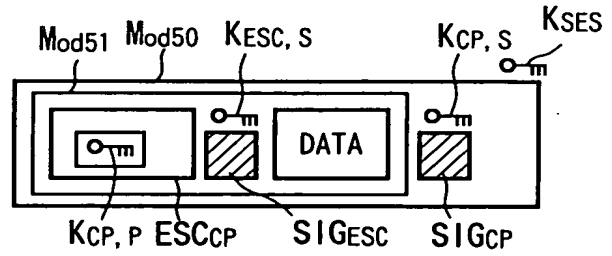


FIG.42B 101 (CP) → SAM105₁
(OUT-OF-BAND)

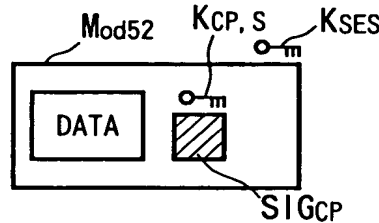


FIG.42C 102 (ESC) → SAM105₁
(OUT-OF-BAND)

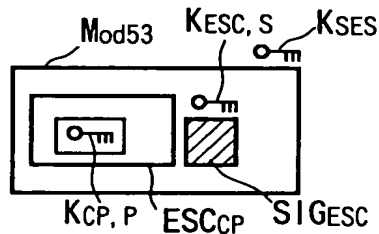


FIG.42D SAM105₁ → 101 (CP)
(IN-BAND)

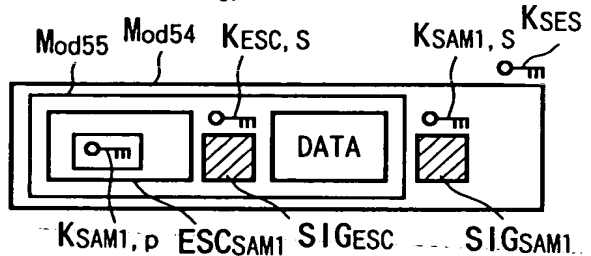


FIG.42E SAM105₁ → 101 (CP)
(OUT-OF-BAND)

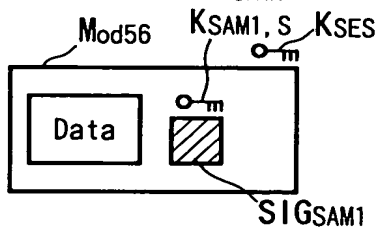


FIG.42F 102 (ESC) → 101 (CP)
(OUT-OF-BAND)

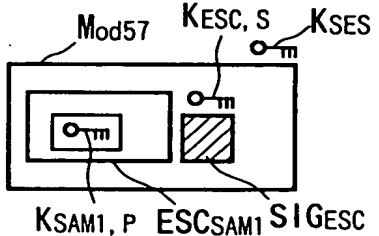


FIG.43G 101 (CP) → 102 (ESC)
(IN-BAND)

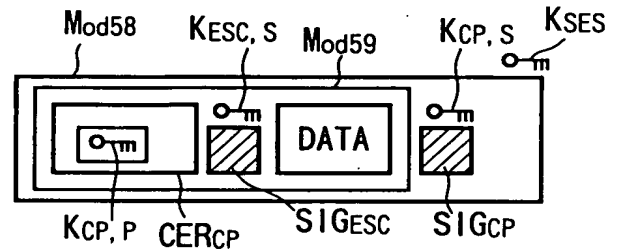


FIG.43H 101 (CP) → 102 (ESC)
(OUT-OF-BAND)

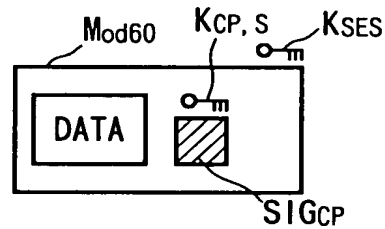


FIG.43I SAM105₁ → 102 (ESC)
(IN-BAND)

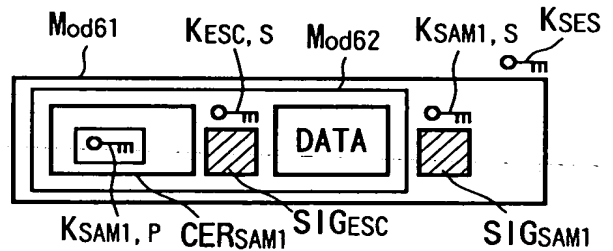


FIG.43J SAM105₁ → 102 (ESC)
(OUT-OF-BAND)

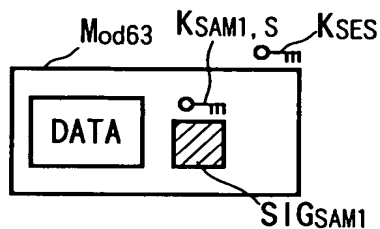


FIG.44

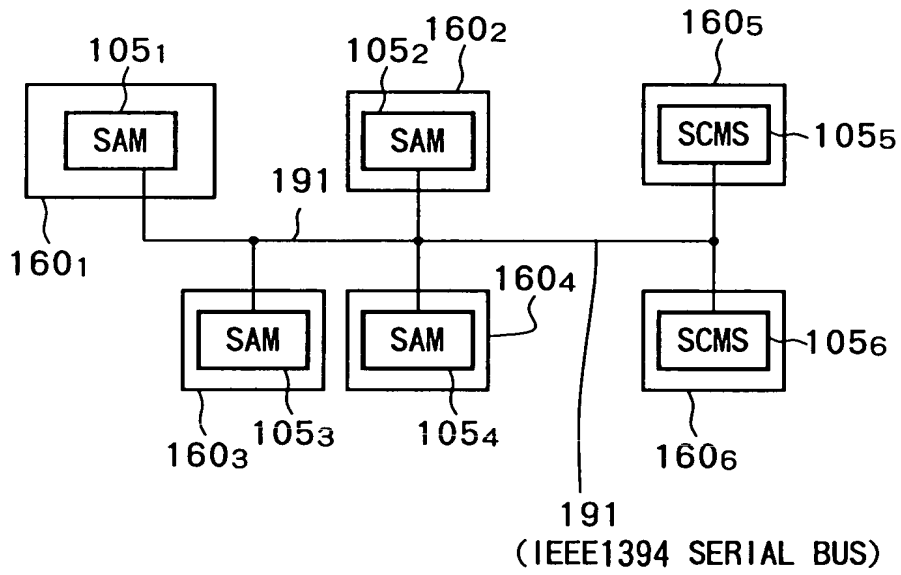
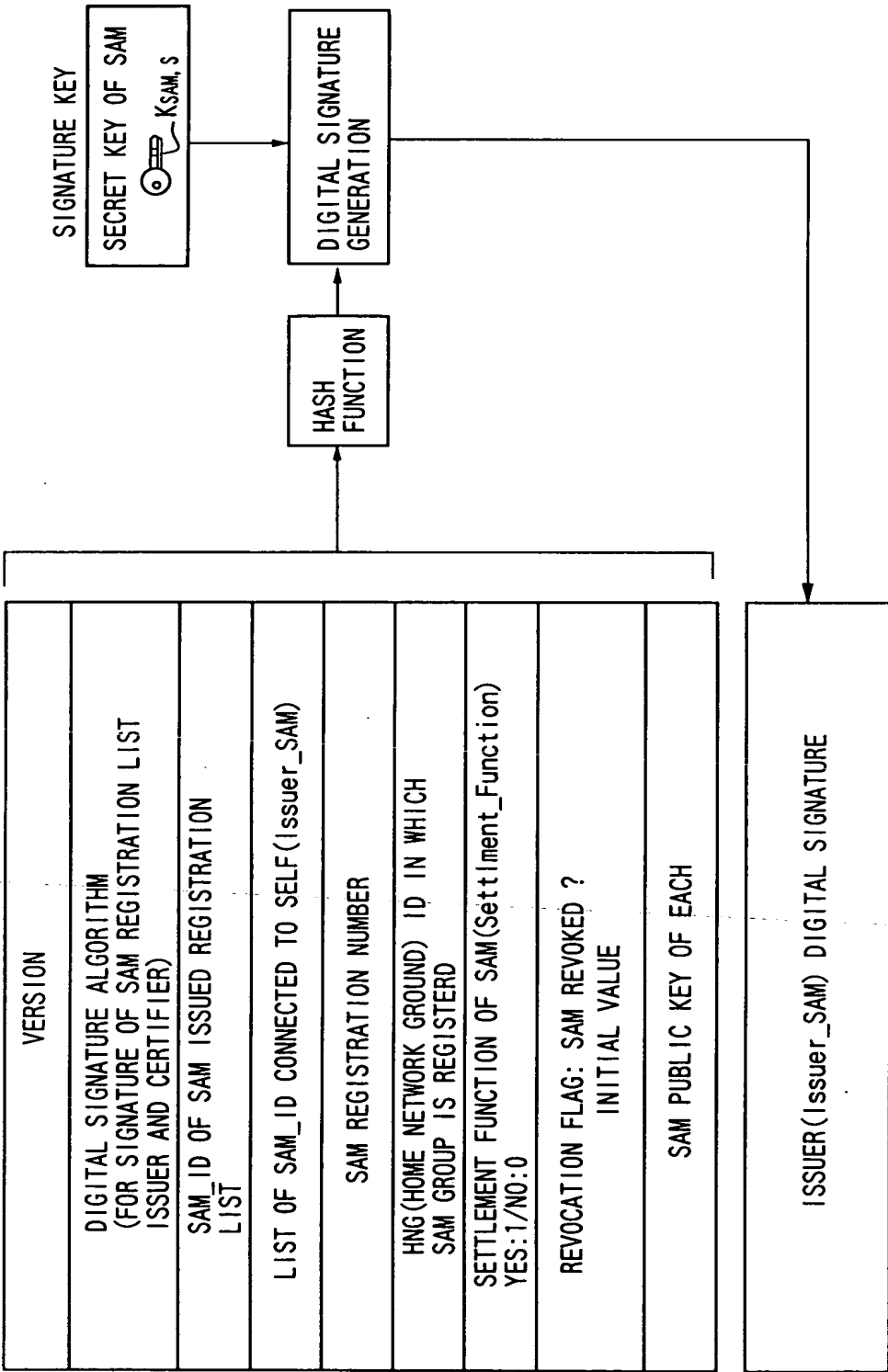


FIG.45

SAM REGISTRATION LIST (PREPARED BY SAM)



SAM REGISTRATION LIST (PREPARED BY EMD SERVICE CENTER)

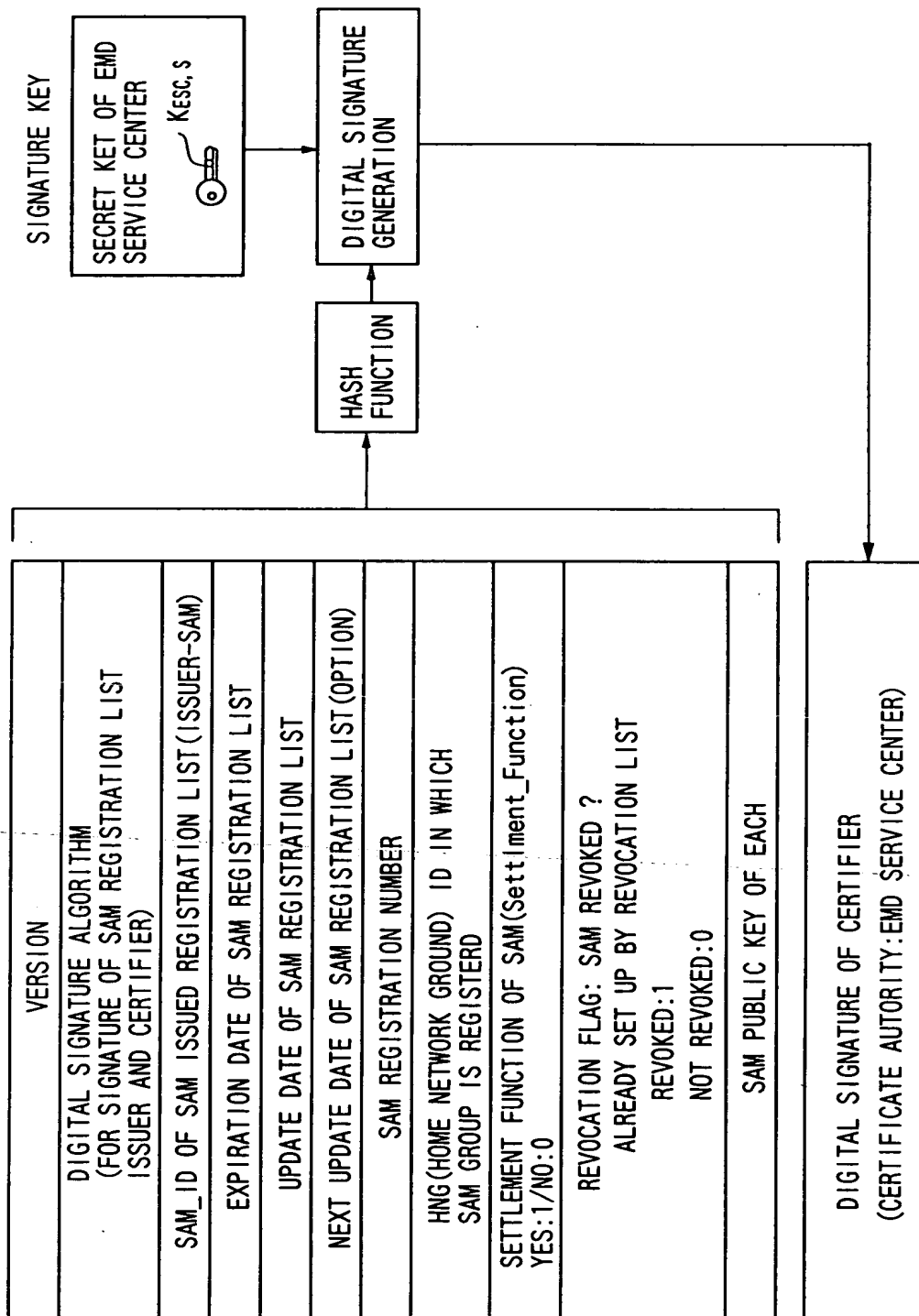


FIG.47

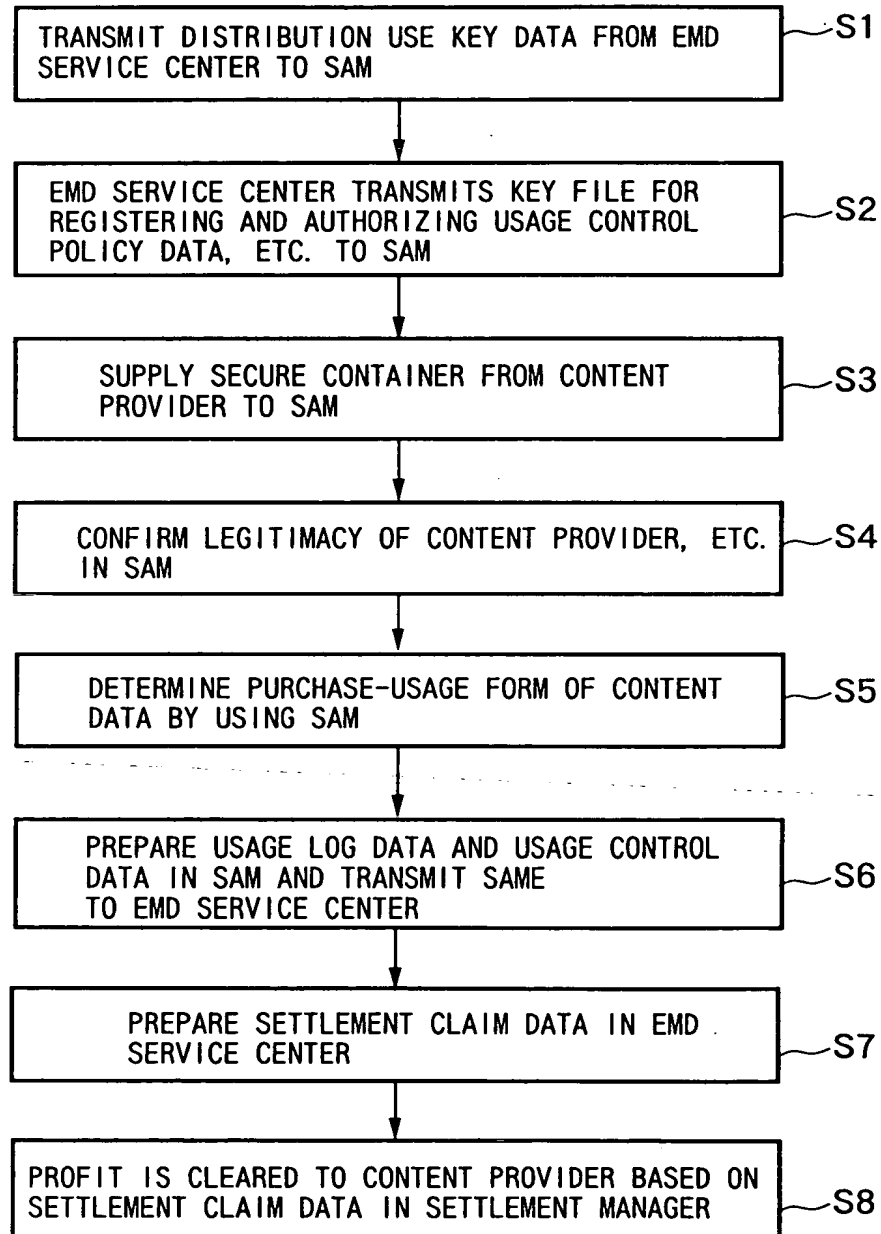


FIG. 48

RETRANSMISSION PROTOCOL FOR REDISTRIBUTION BETWEEN HOME EC/APPARATUS

RETRANSMISSION PROTOCOL FOR REDISTRIBUTION BETWEEN HOME EC/APPARATUS

CONTENT PROVIDER USE TRANSPORT PROTOCOL

IN HOME EC/DISTRIBUTION SERVICE XML/SMIL ON 1394

BETWEEN HOME EC/ DISTRIBUTION SERVICE XML/SMIL ON 1394

REDISTRIBUTION BETWEEN APPARATUSES (IN HOME) STORAGE MEDIUM→STORAGE MEDIUM

REDISTRIBUTION BETWEEN APPARATUSES (BETWEEN HOMES) STORAGE MEDIUM→STORAGE MEDIUM

SECURE CONTAINER 104

CONTENT PROVIDER 101

INTERNET XML/SMILON TCP/IP

ROUTE CERTIFICATE AUTHORITY 90

EMD SERVICE CENTRE 102

PAYMENT GATEWAY

SETTLEMENT MANAGER

USAGE STATEMENT

SMALL SUM SETTLEMENT

103 USER HOME NETWORK

103a

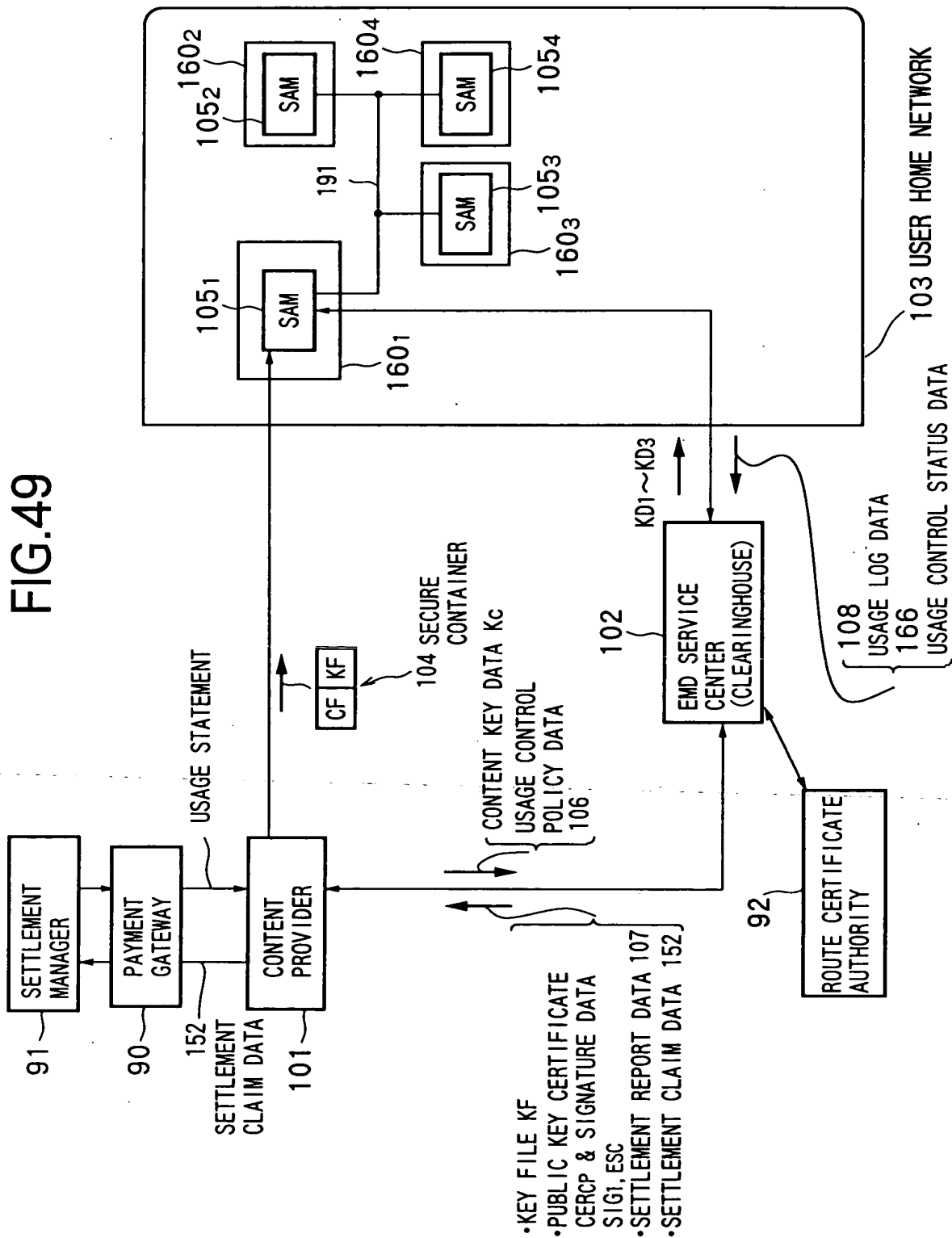
103b

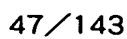
1394

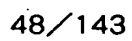
008 (Out-Of-Band) (KEY FILE)

In-Band kf (KEY FILE)

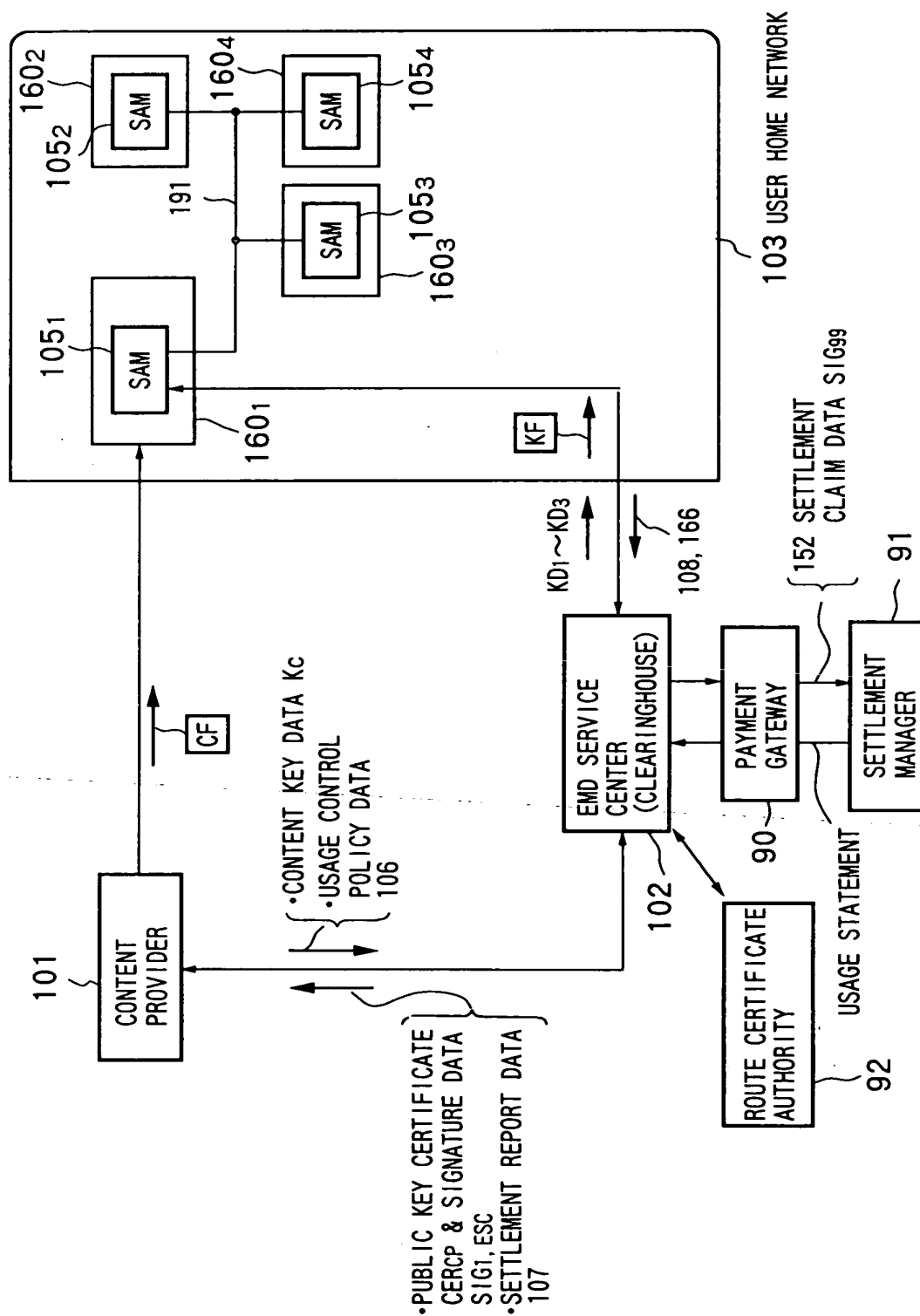
RIGHT REGISTRATION OF CONTENT

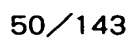




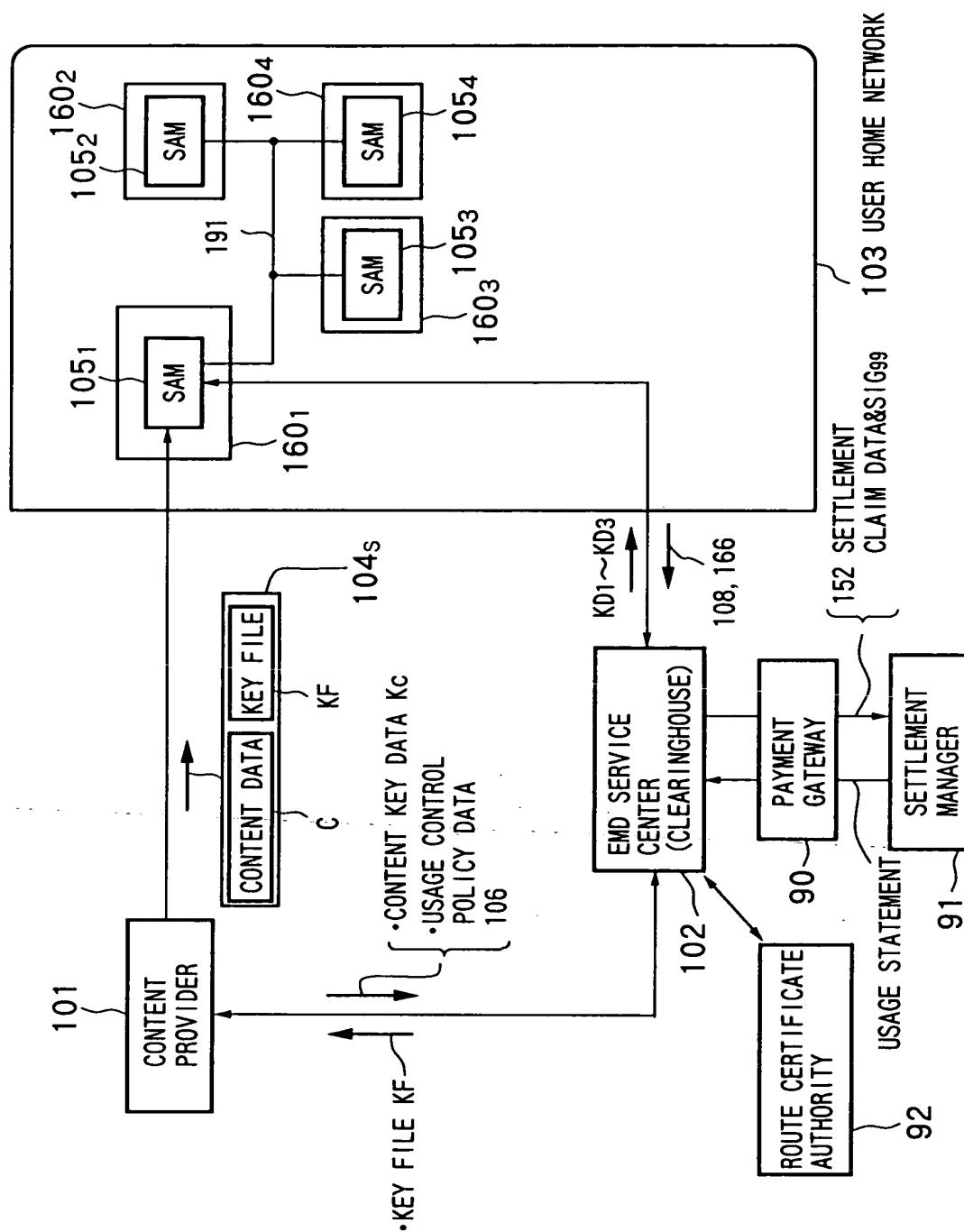


49/143





51/143



53/143

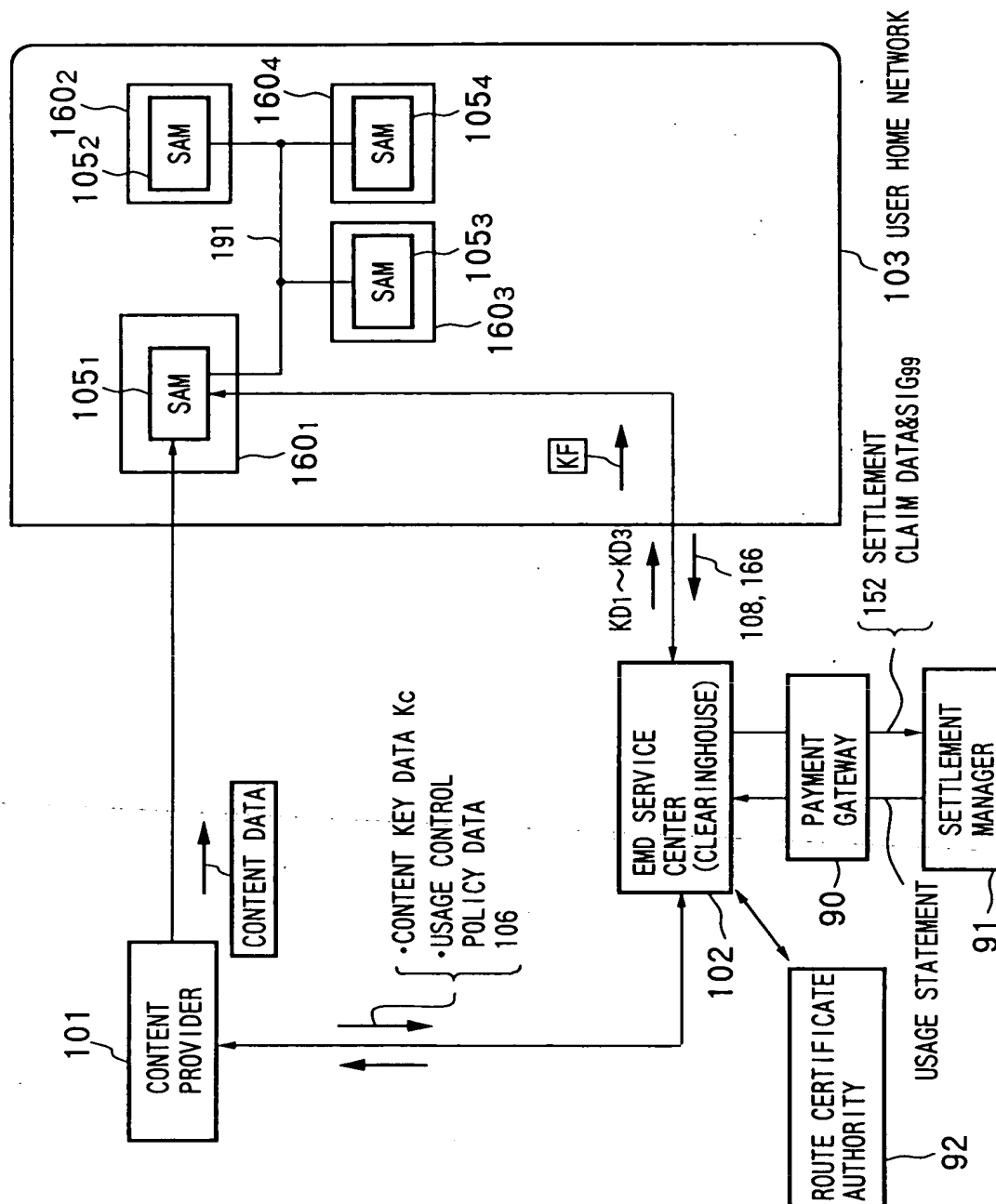


FIG. 57

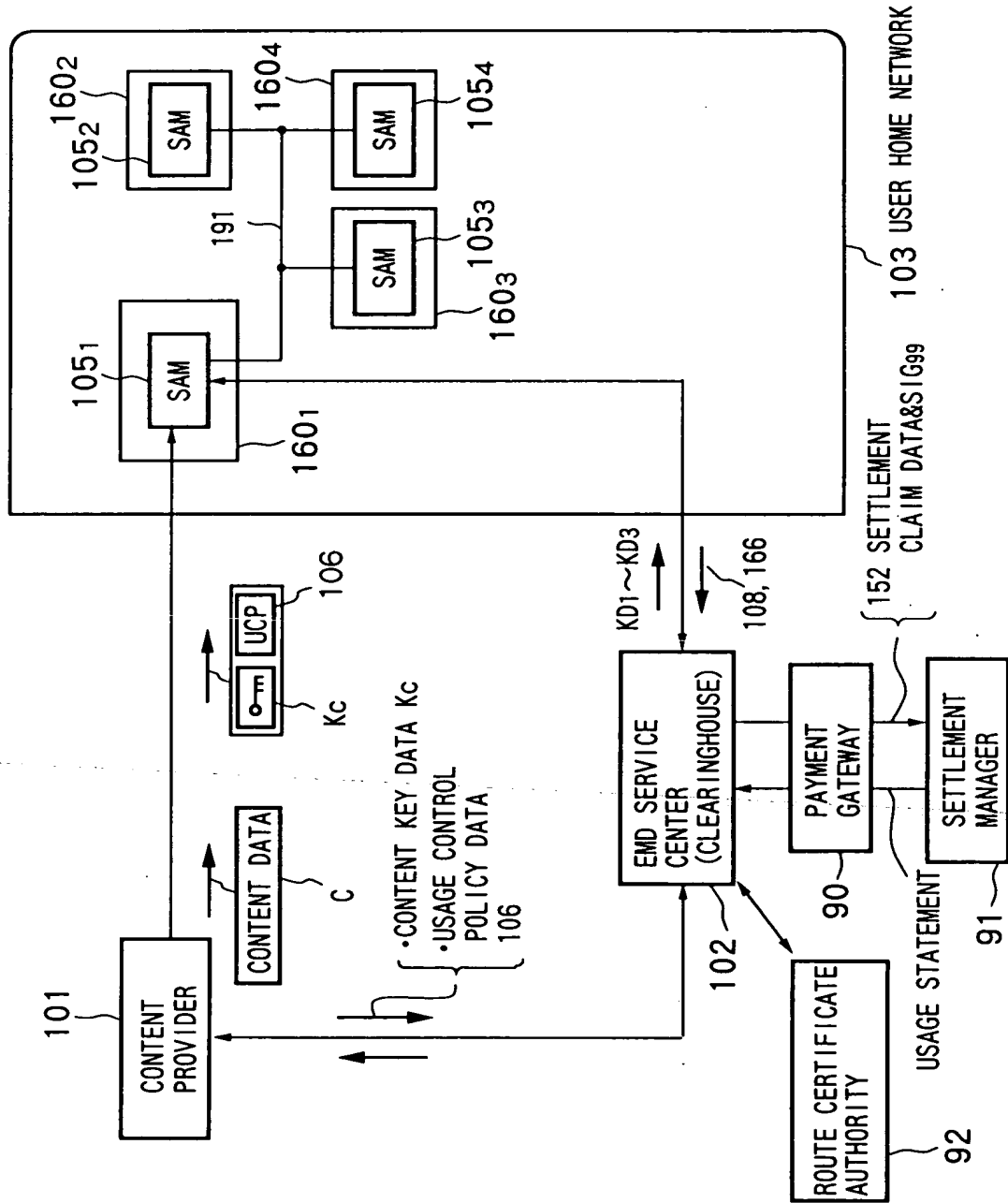


FIG. 58

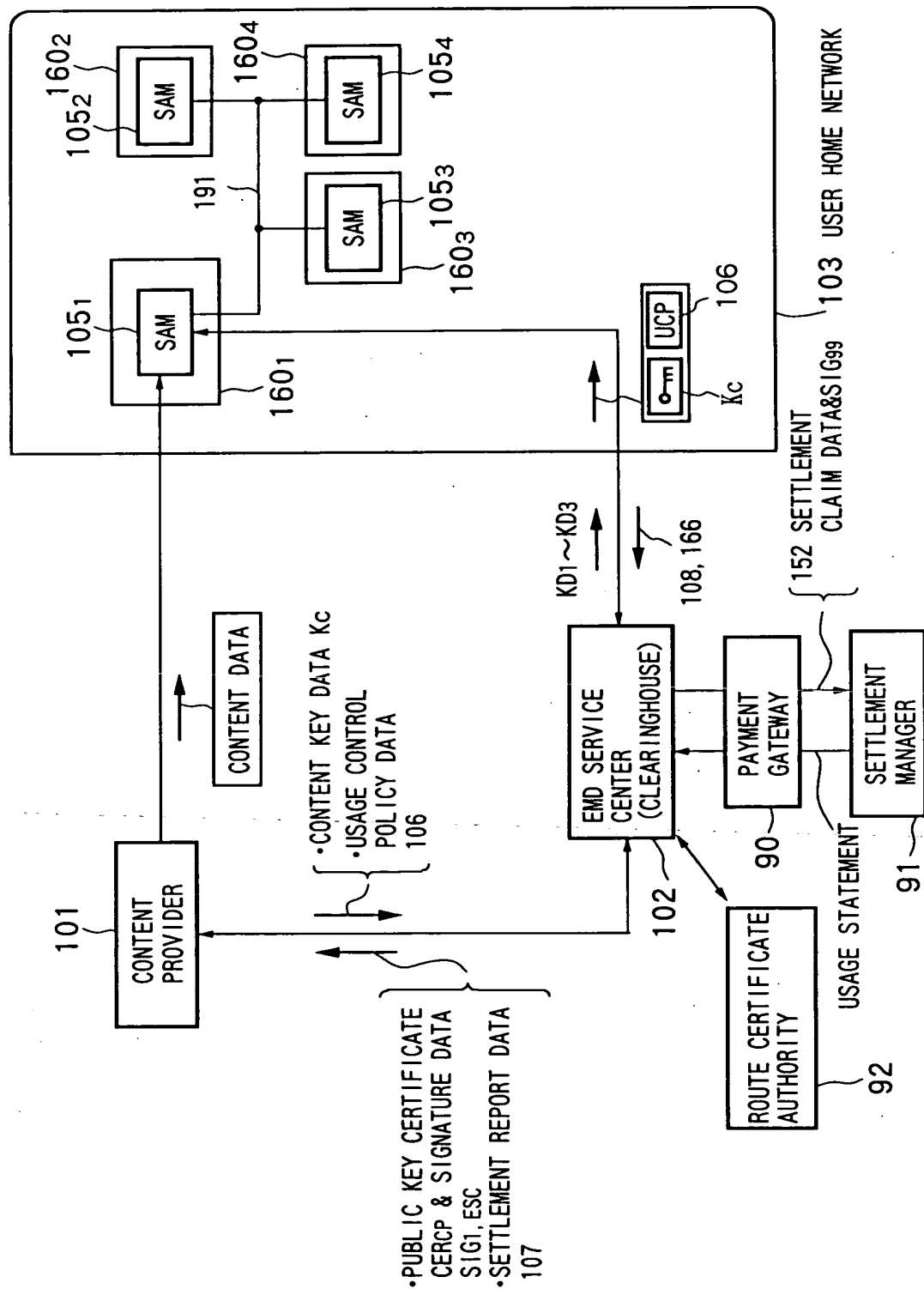
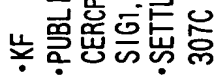


FIG. 59



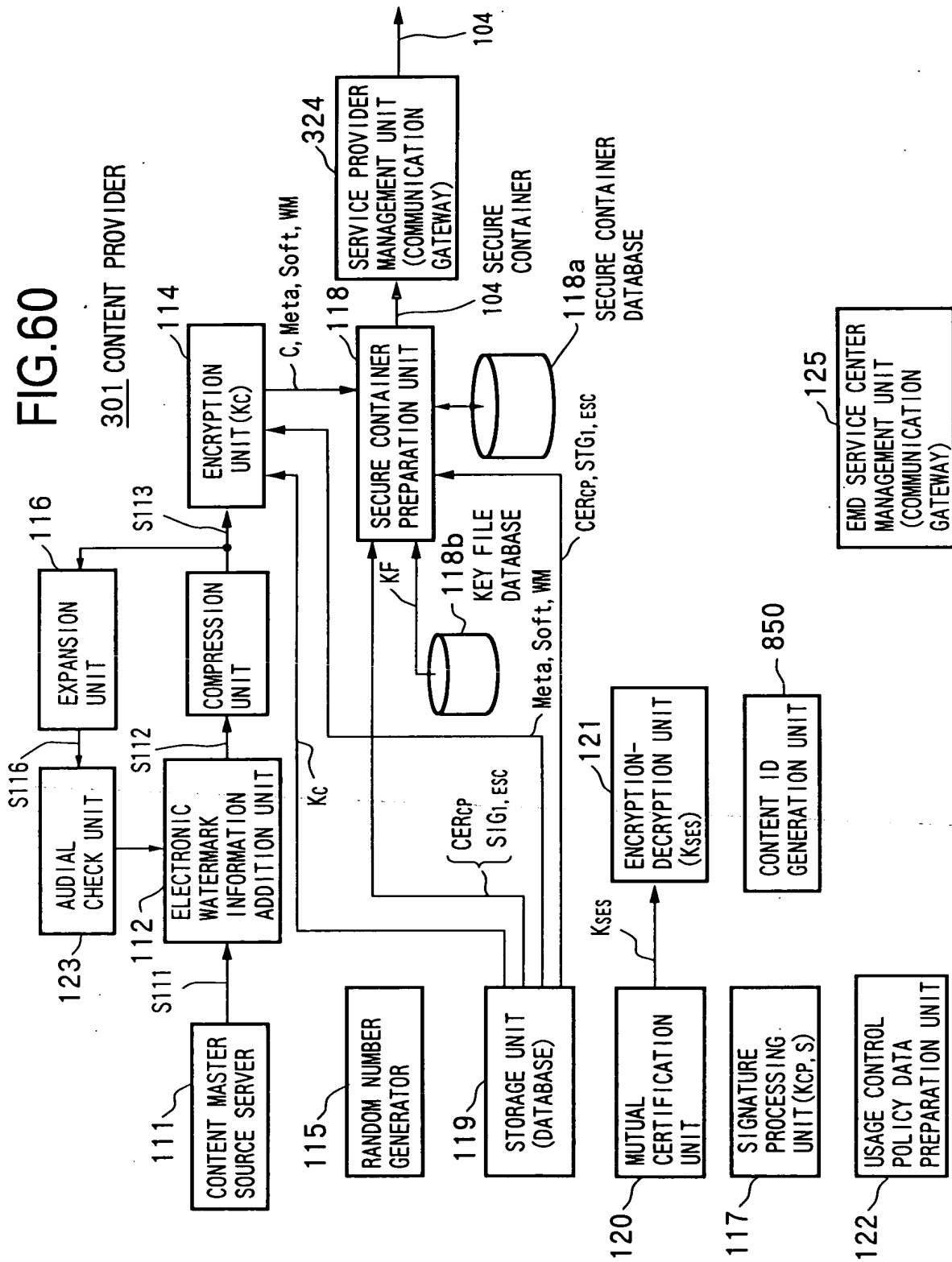


FIG.61

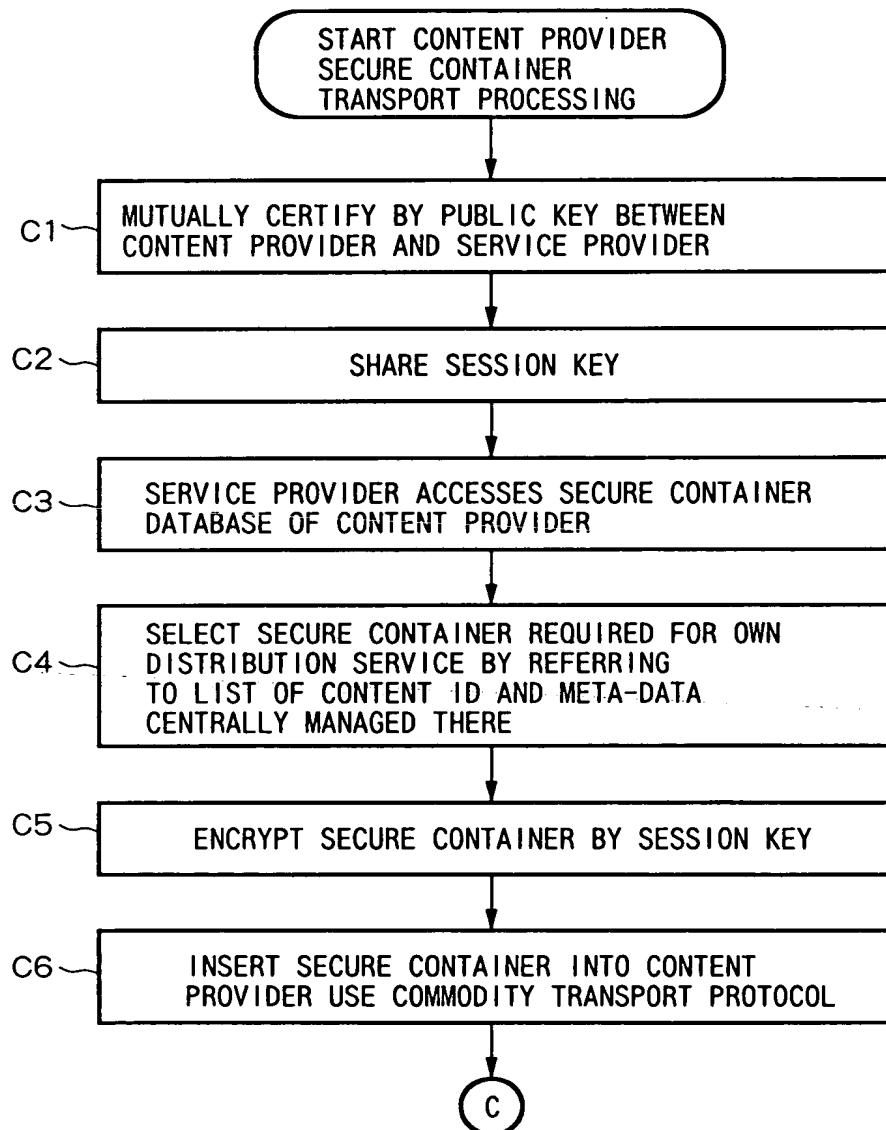
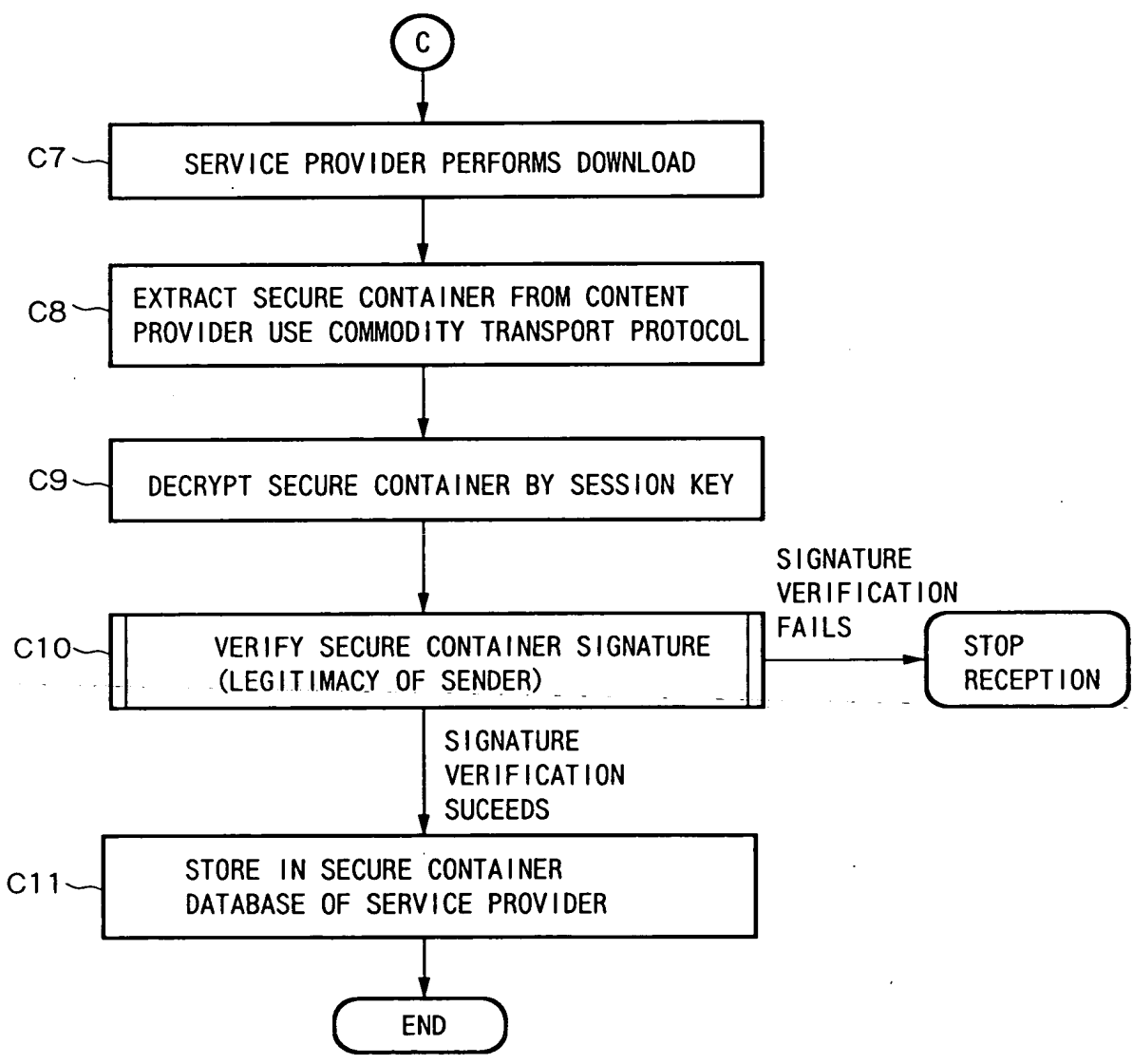


FIG.62



09/856276 1.00201

FIG. 63

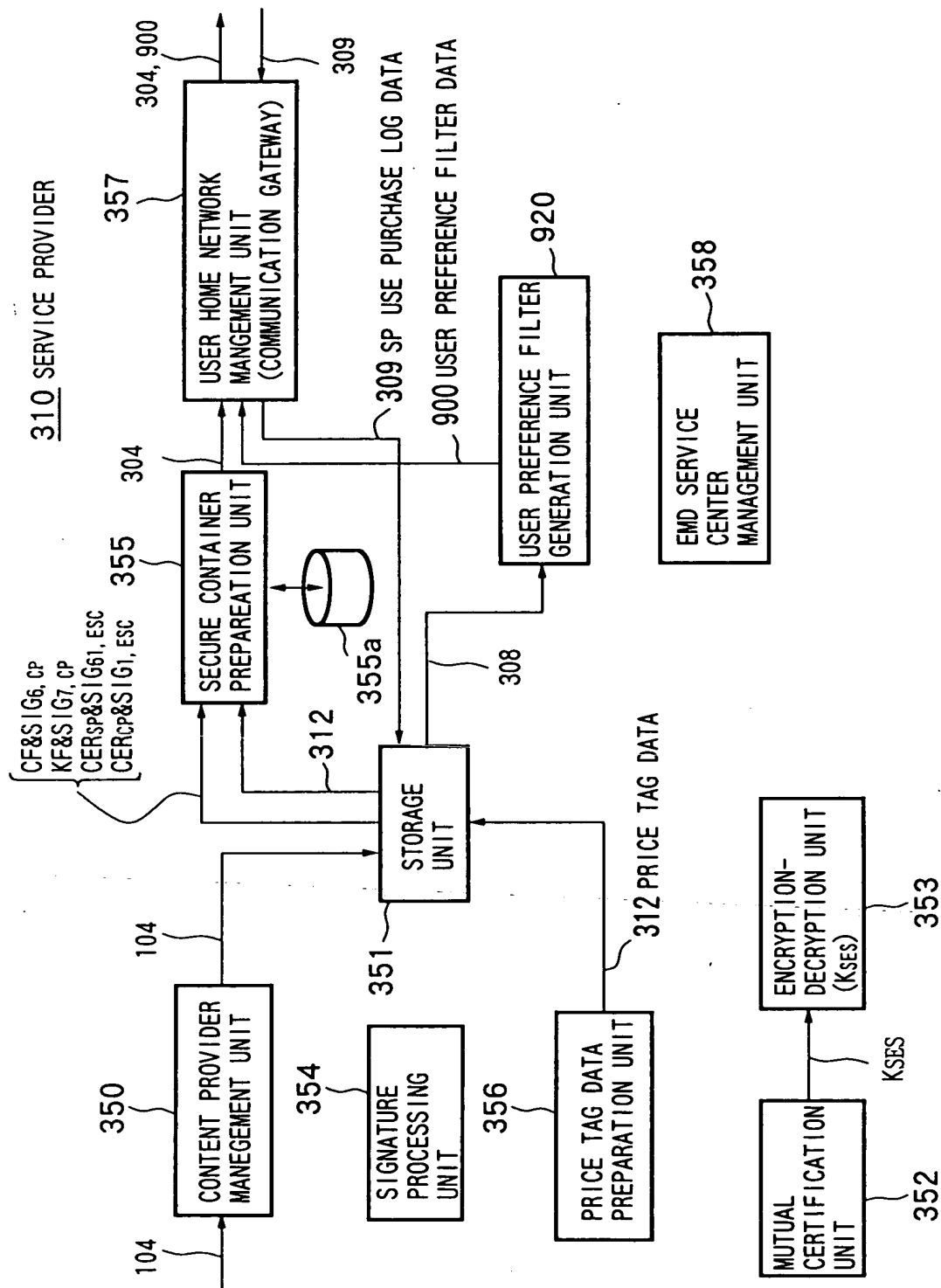
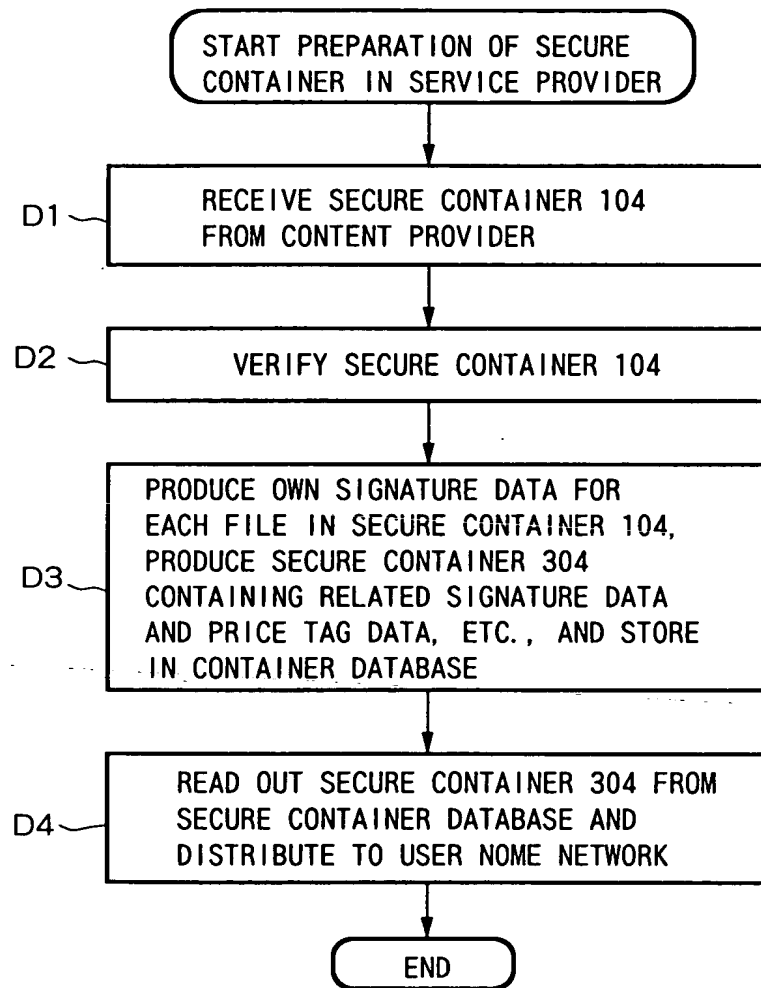


FIG.64



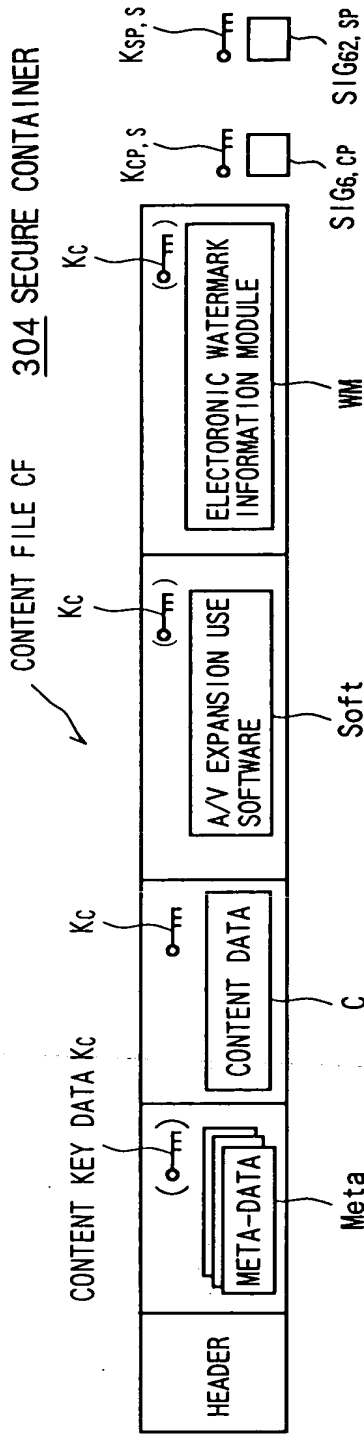


FIG. 65A

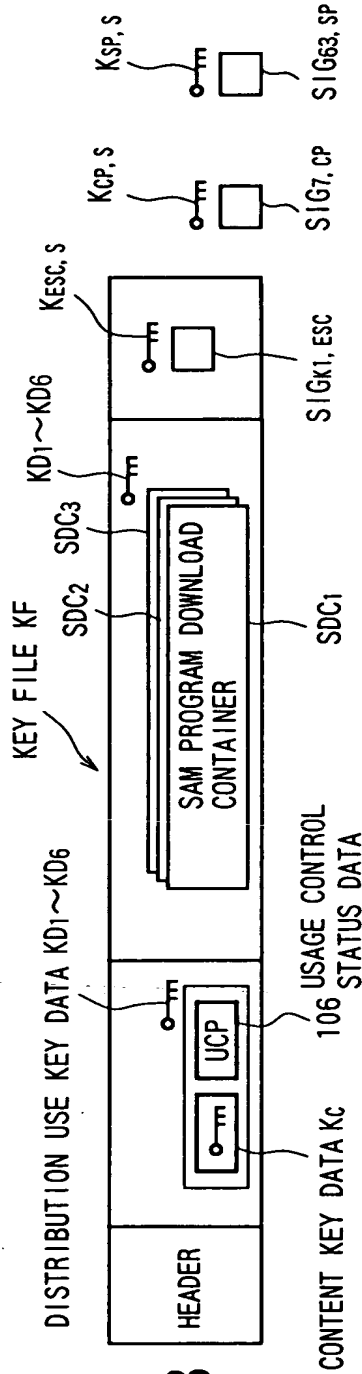


FIG. 65B

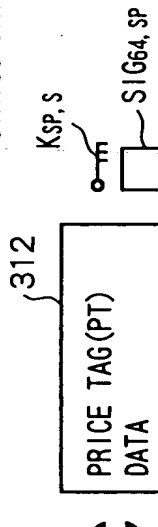


FIG. 65C

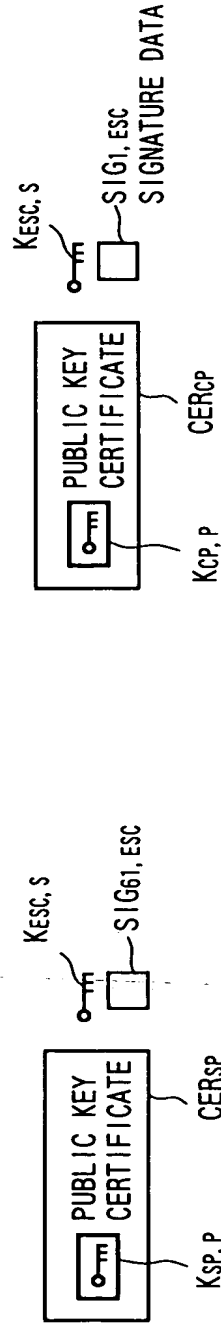


FIG. 65D

FIG.66

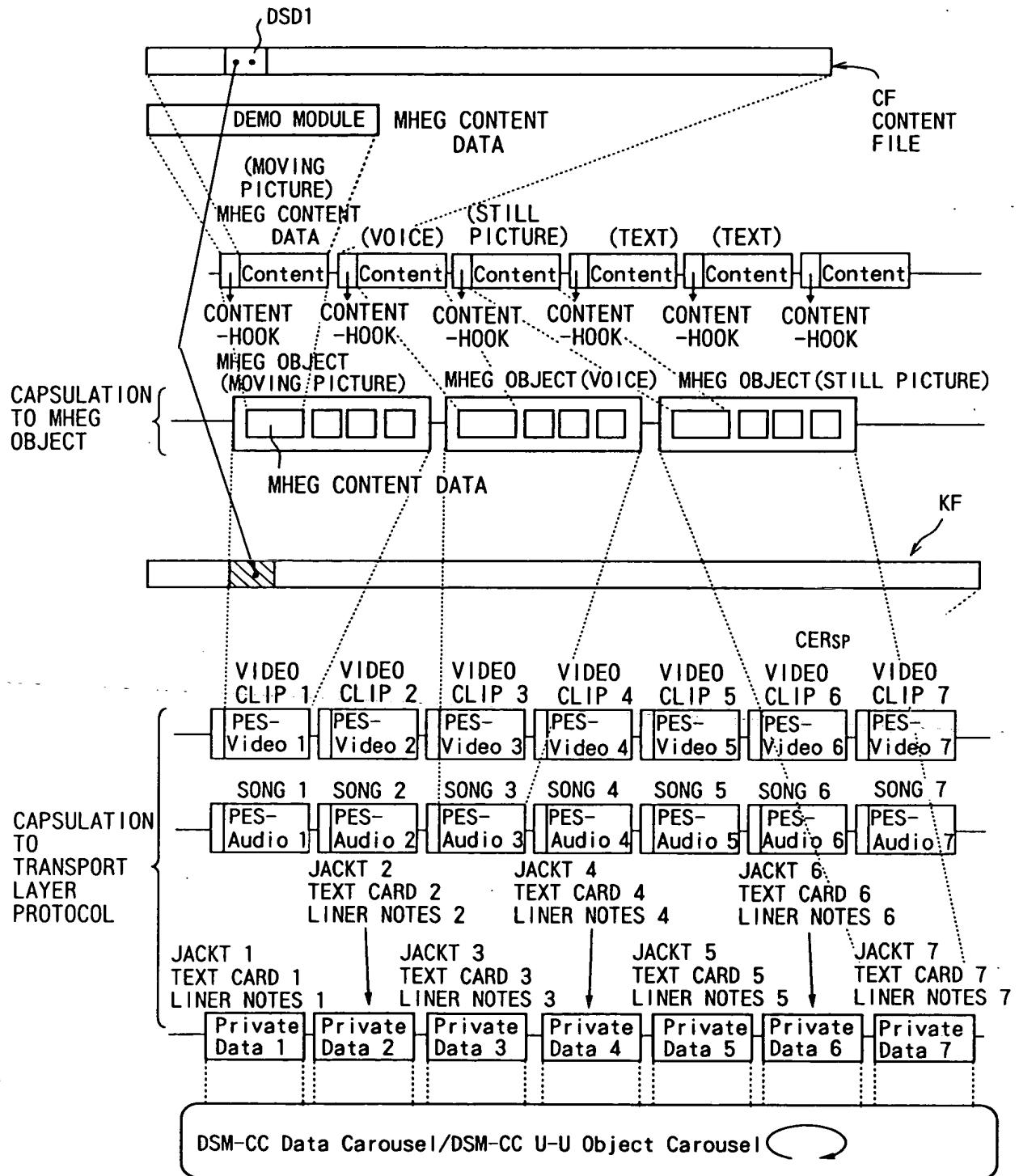


FIG.67

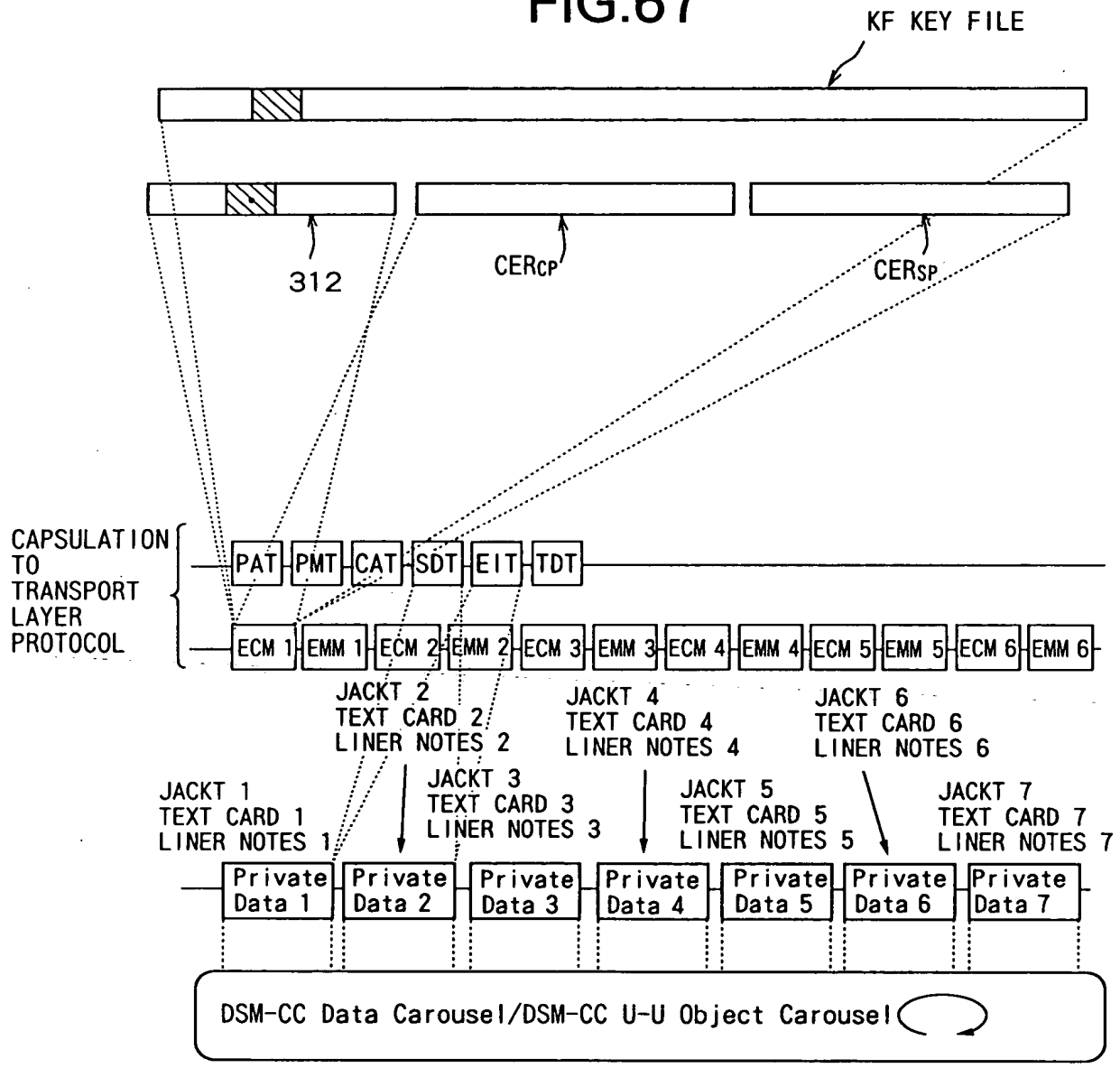


FIG.68

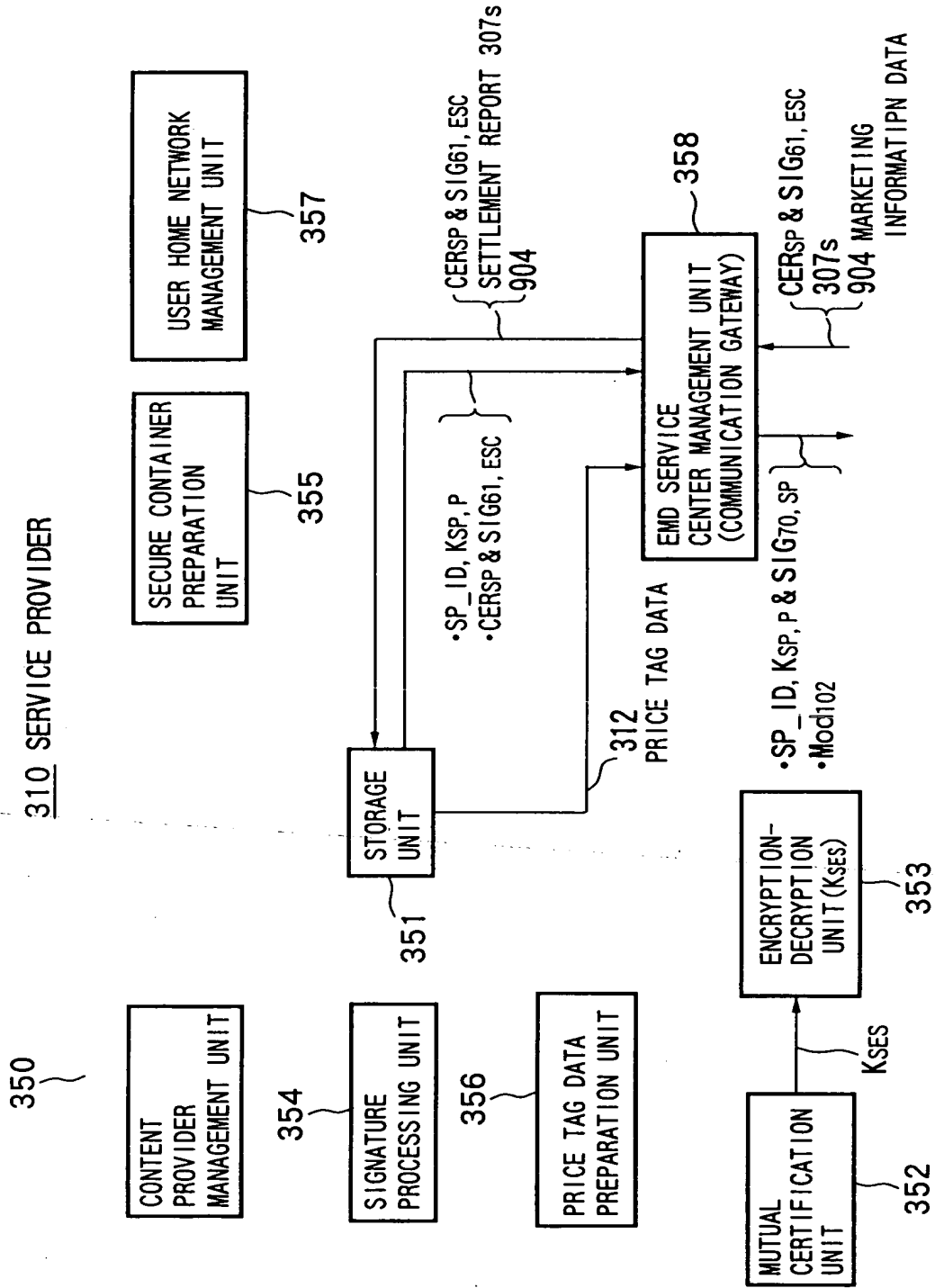
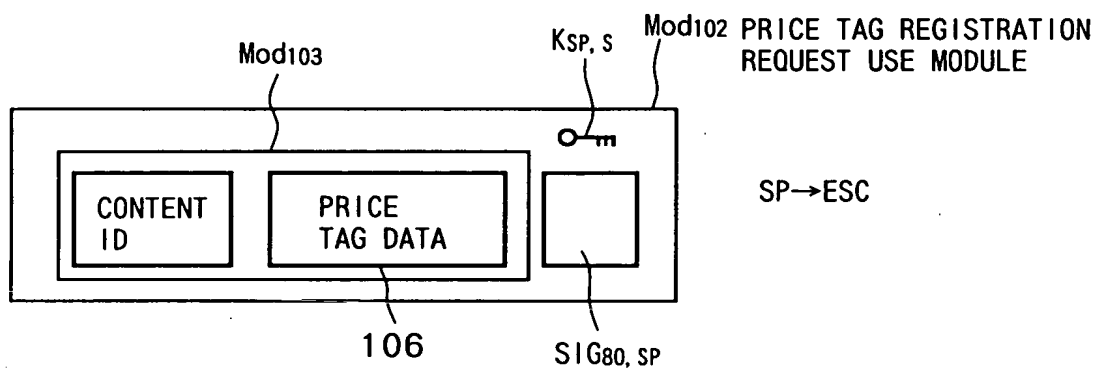


FIG.69



67/143

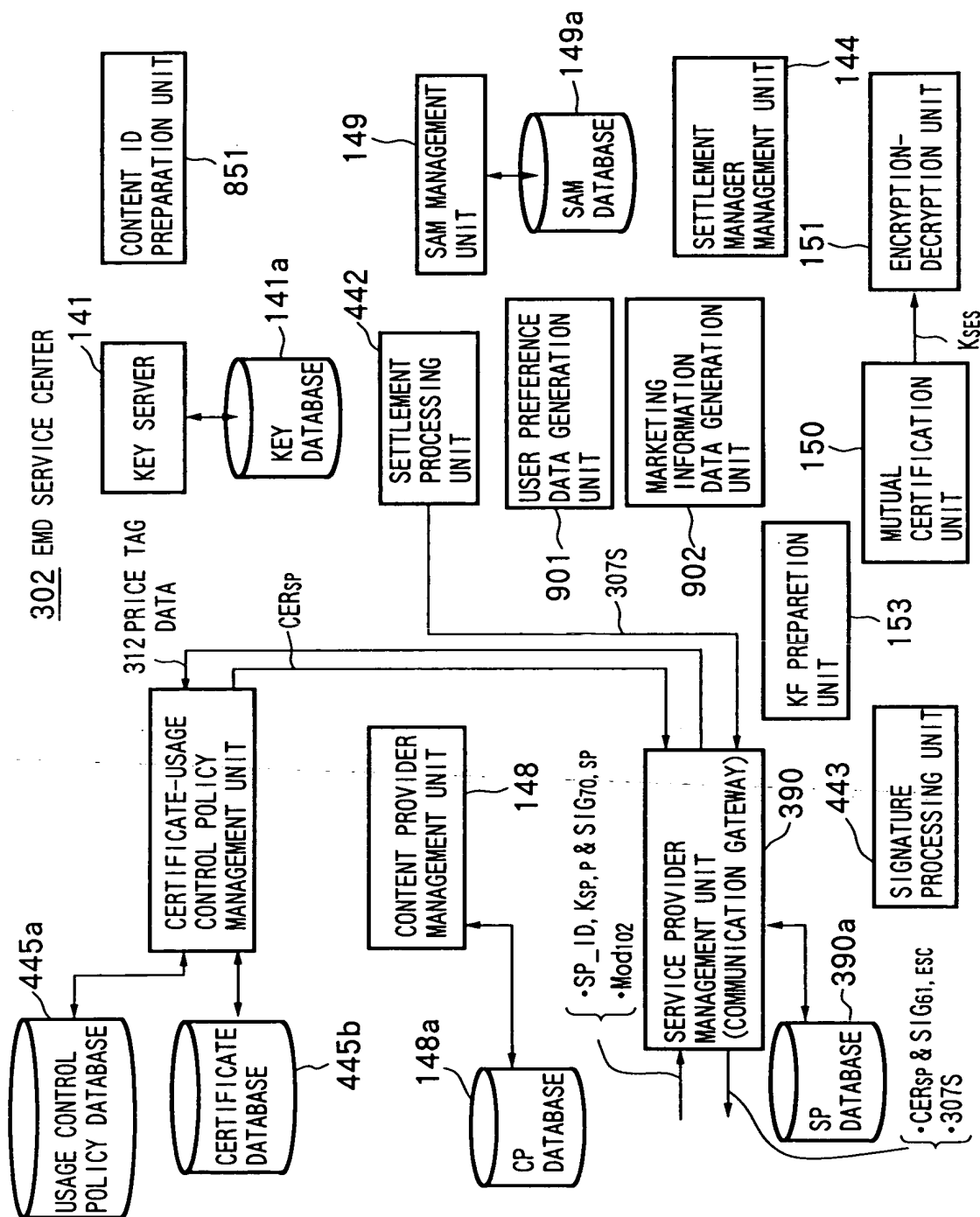
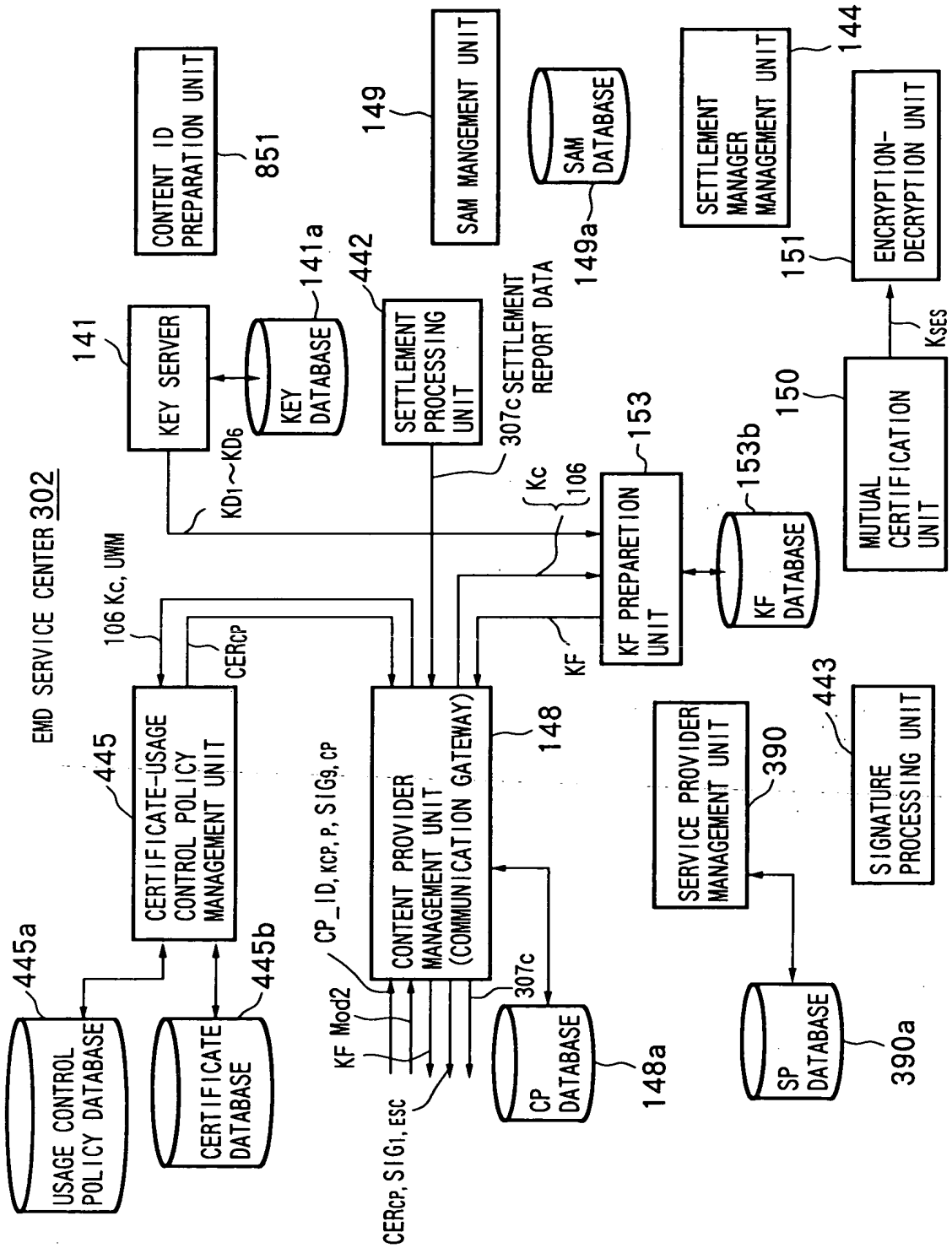


FIG. 71



[illegible]

FIG.73**CONTENT OF USAGE LOG DATA 308****IDENTIFIER Content_ID****IDENTIFIER CP_ID****IDENTIFIER SP_ID****SIGNAL PARAMETER DATA OF CONTENT DATA C****COMPRESSION METHOD OF CONTENT DATA C****IDENTIFIER MEDIA_ID OF STORAGE MEDIA****IDENTIFIER SAM_ID****USER_ID OF USER**

FIG.74

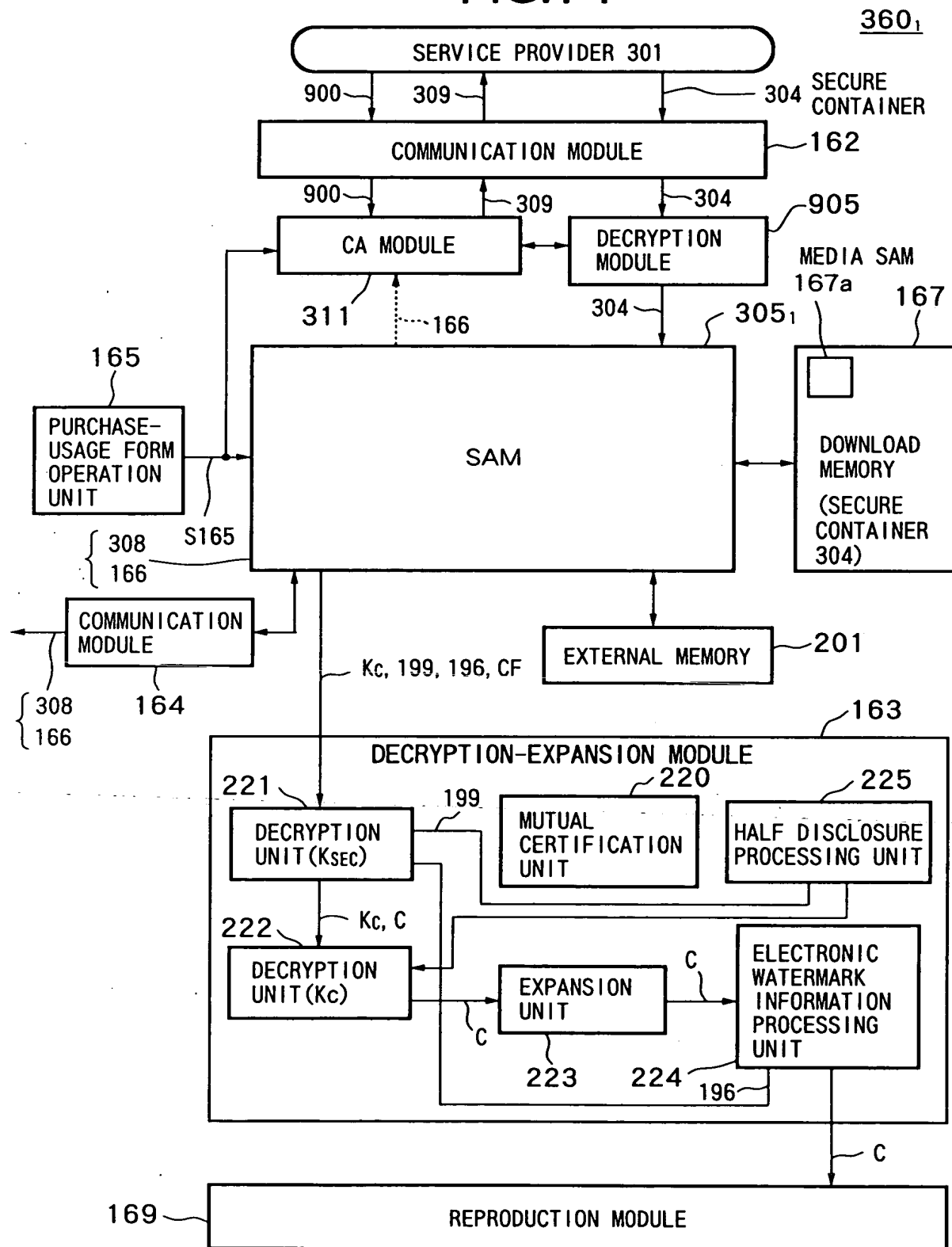


FIG. 75

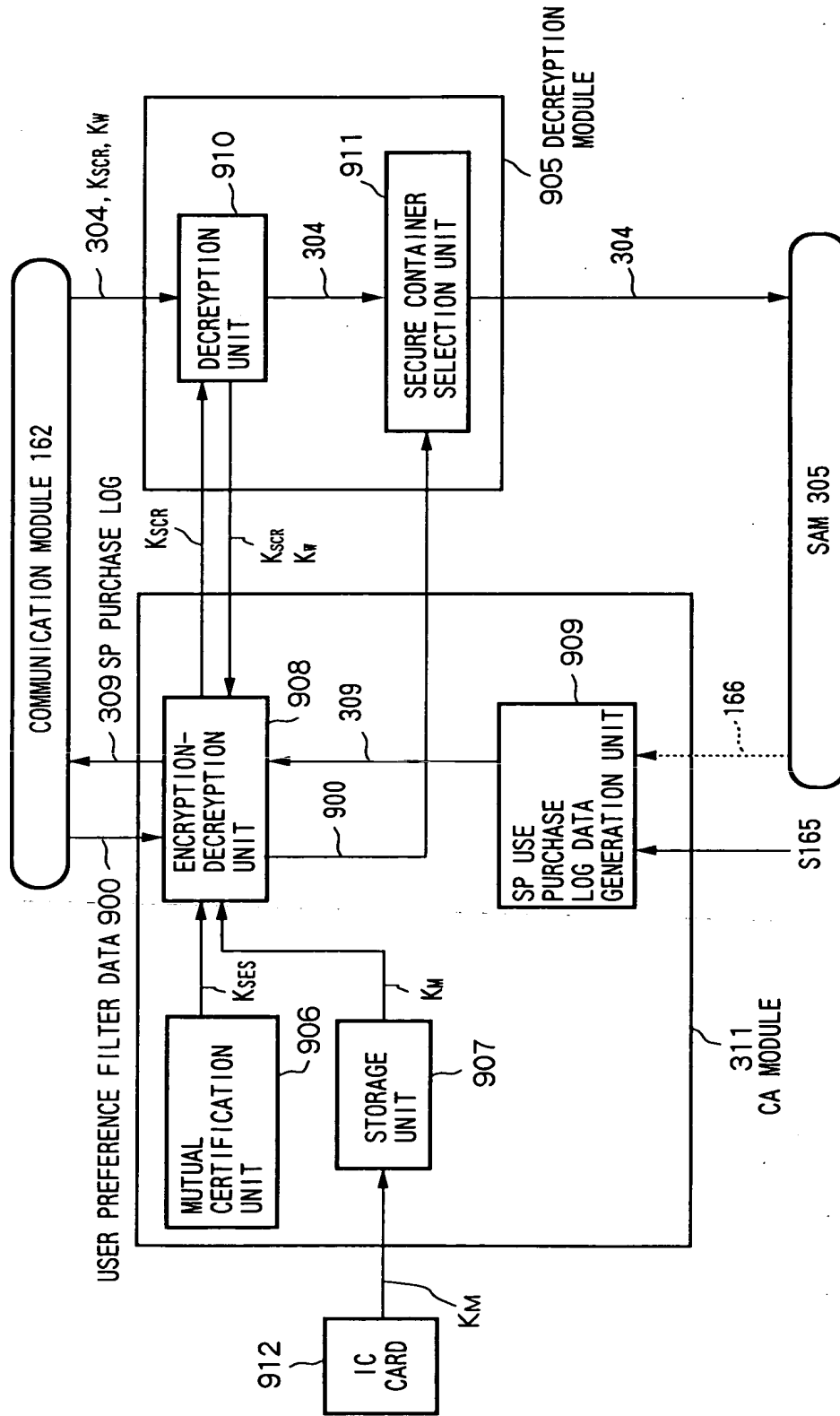


FIG. 76

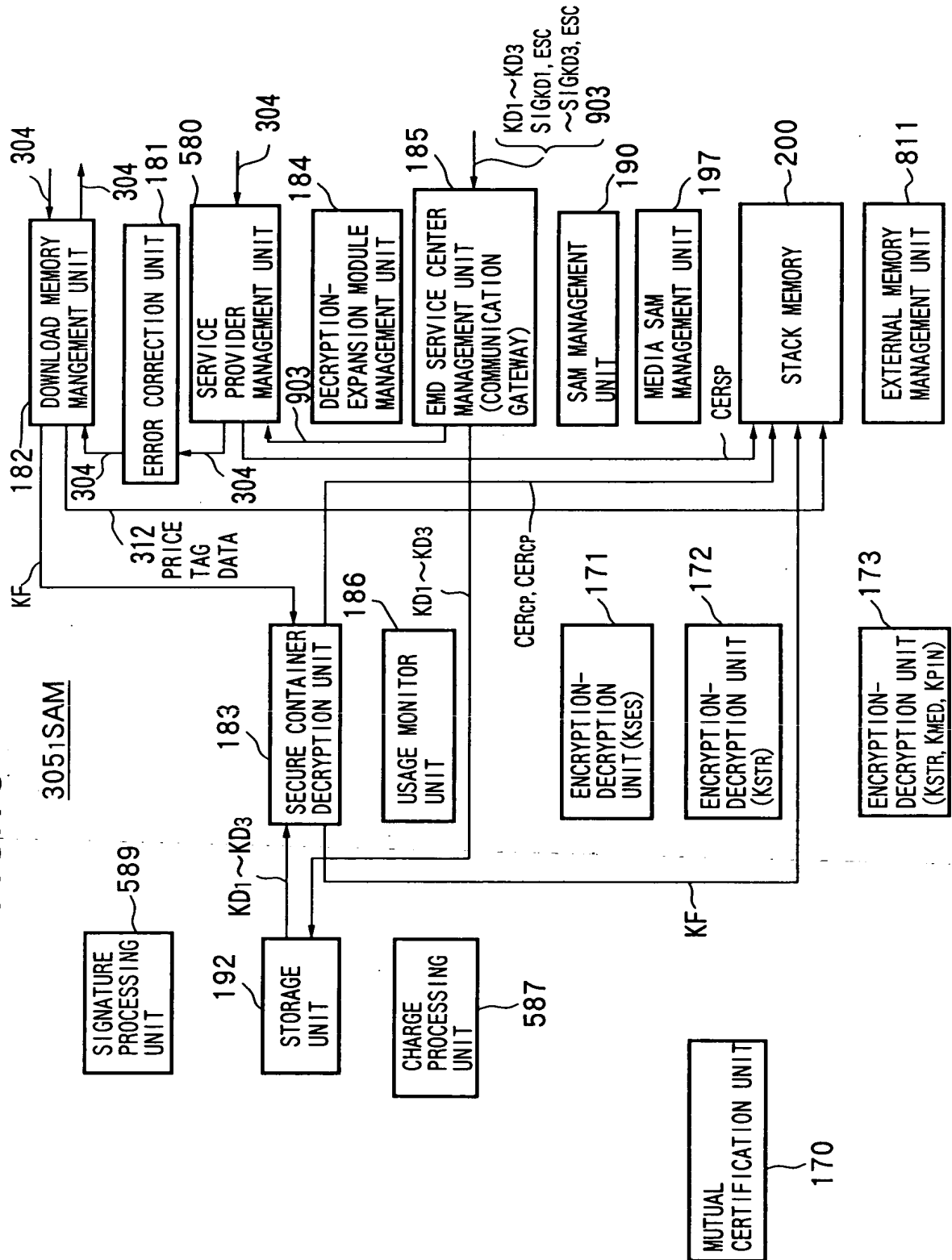


FIG.77

STORED DATA OF STACK MEMORY 200

CONTENT KEY DATA K_c
 USAGE CONTROL POLICY DATA(UCP) 106
 LOCK KEY DATA K_{Loc} OF NOVOLATILE MEMORY 201
 PUBLIC KEY CERTIFICATE DATA CER_{CP} OF CONTENT PROVIDER 301
 PUBLIC KEY CERTIFICATE DATA CER_{SP} OF SERVICE PROVIDER 301
 USAGE CONTROL STATUS DATA(UCS) 166
 SAM PROGRAM DOWNLOAD CONTAINERS $SD_1 \sim SDC_3$
 PRICE TAG DATA 312

FIG. 78

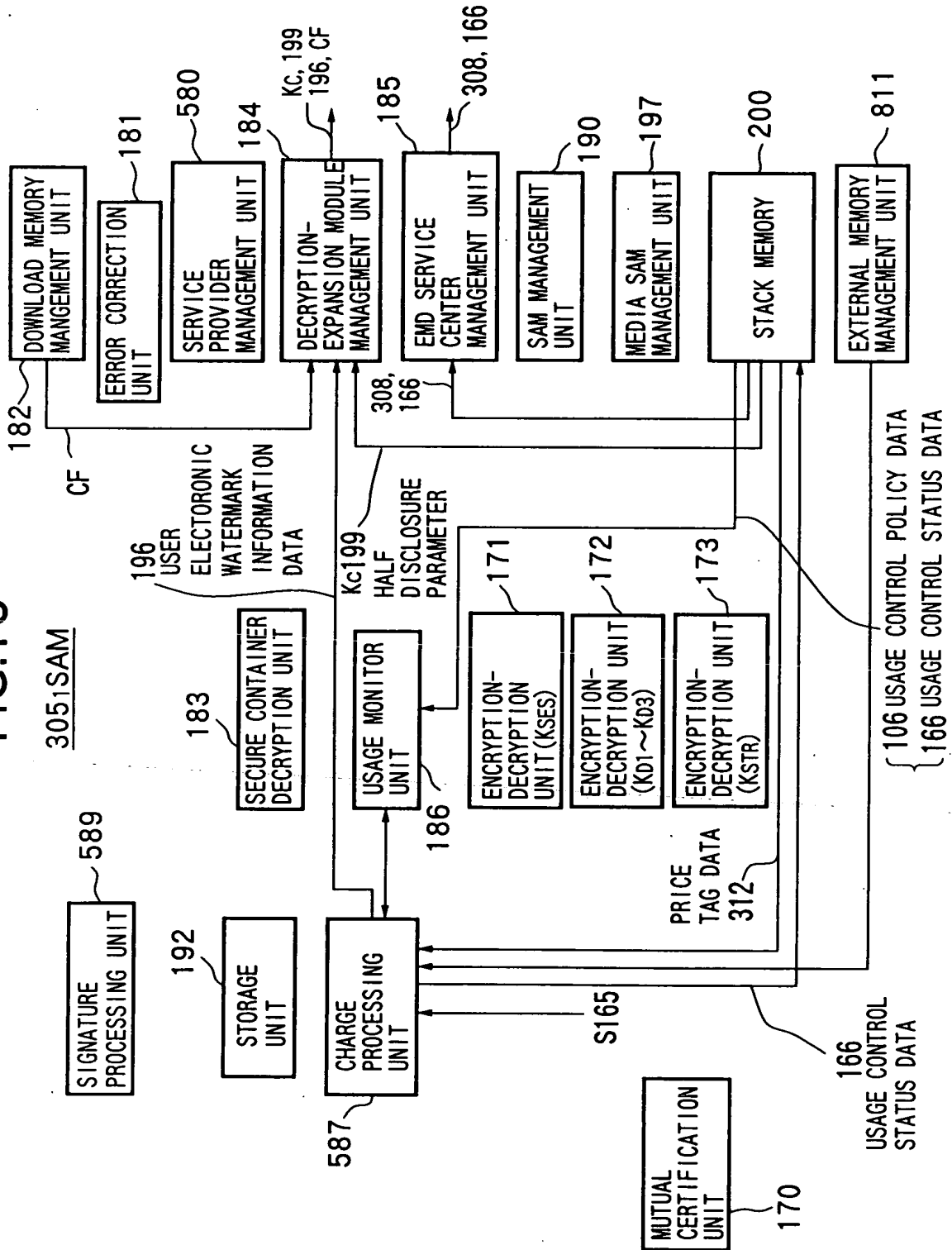


FIG.79

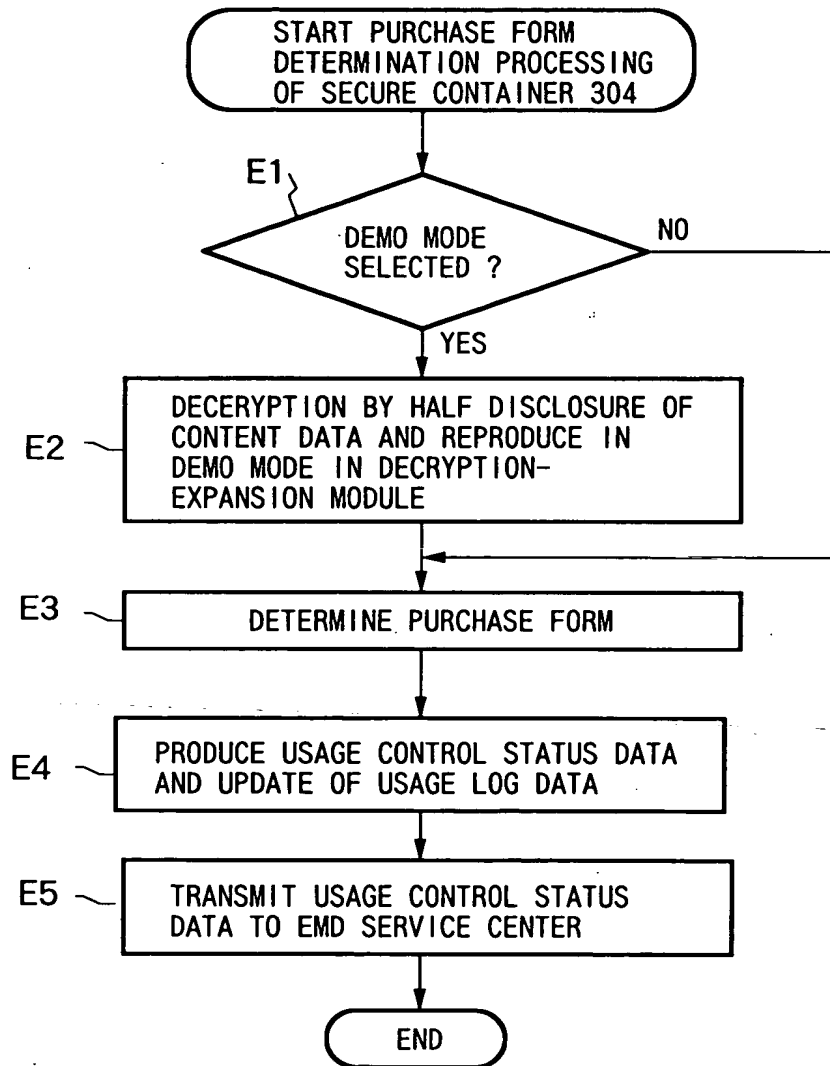


FIG. 80

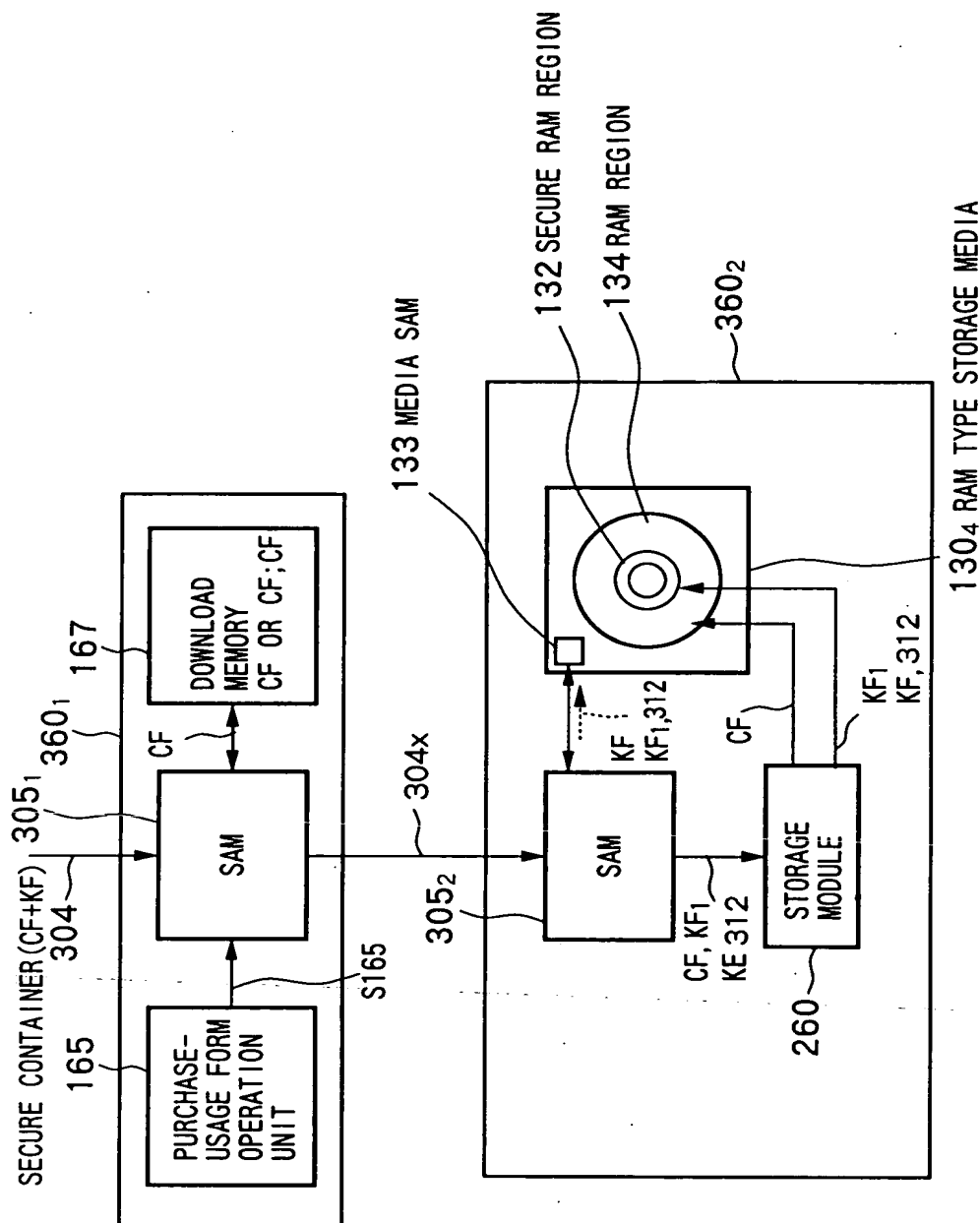
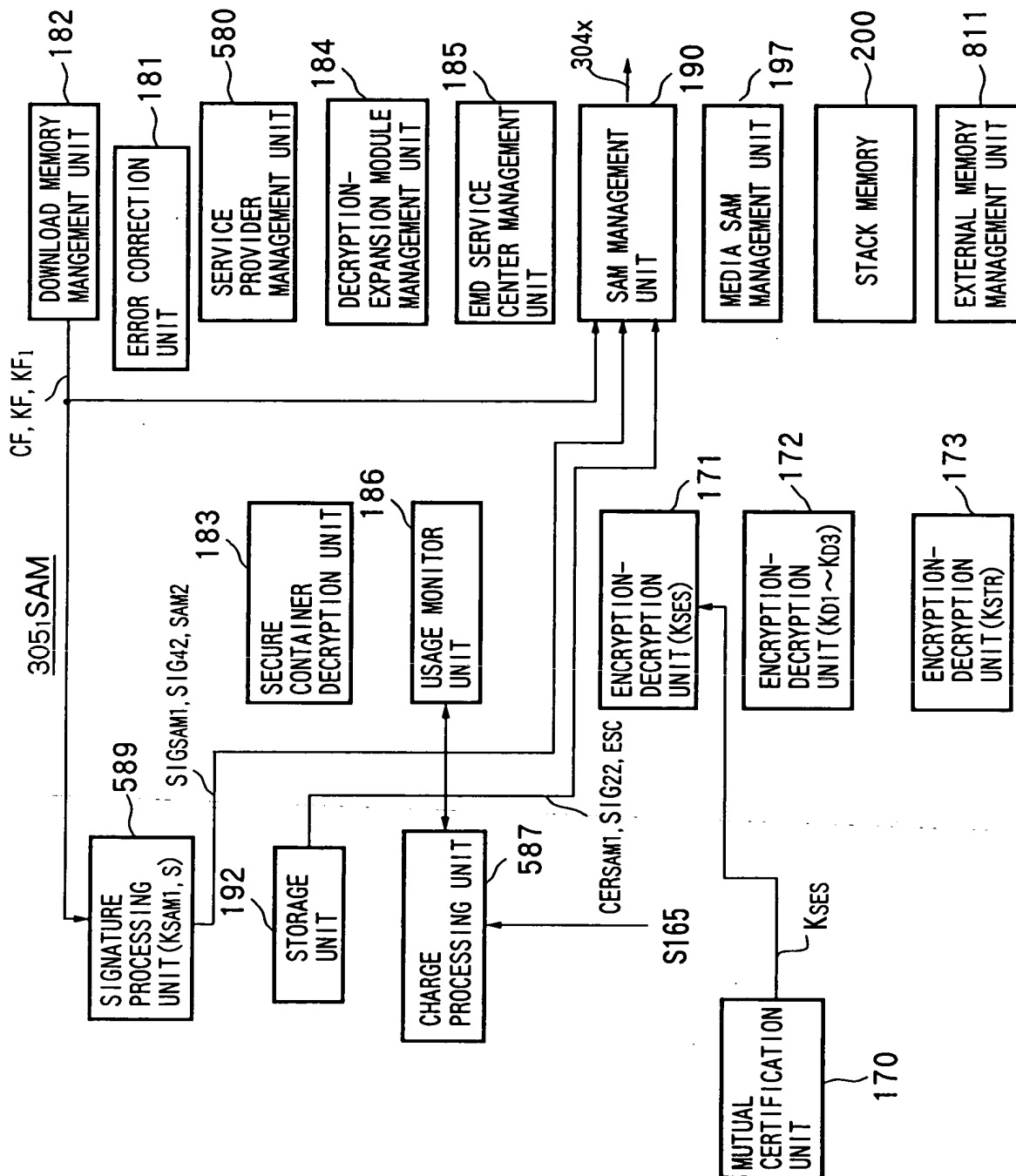




FIG.82



305₂SAM

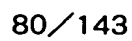


FIG.84

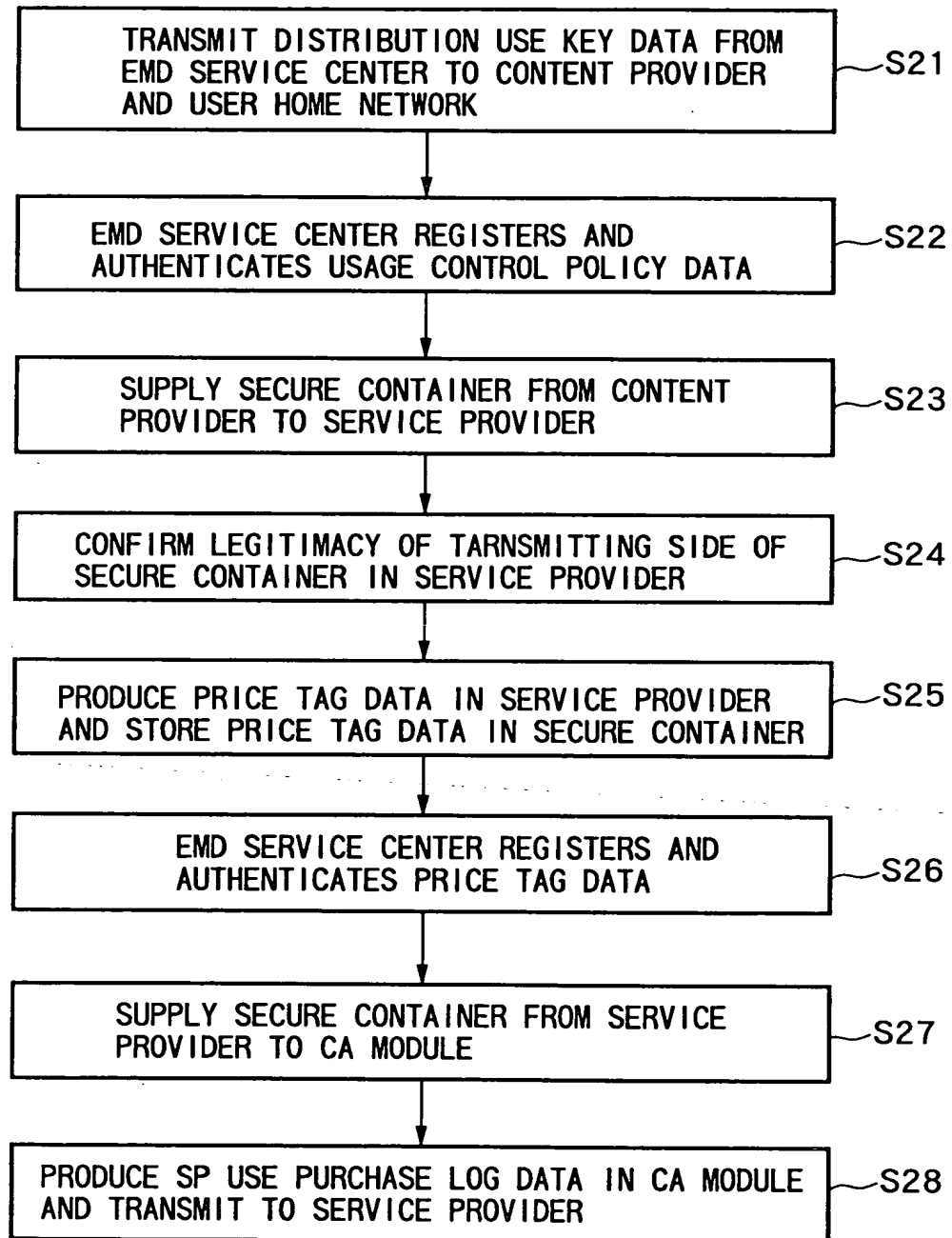


FIG.85

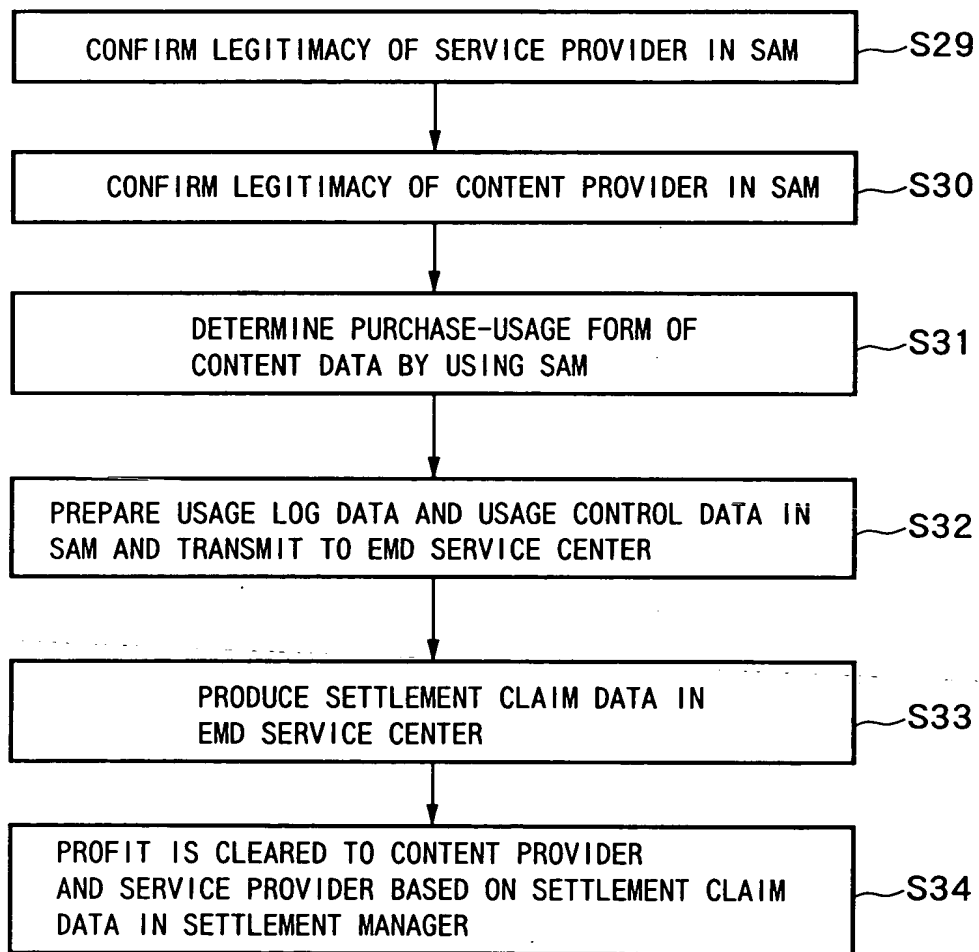
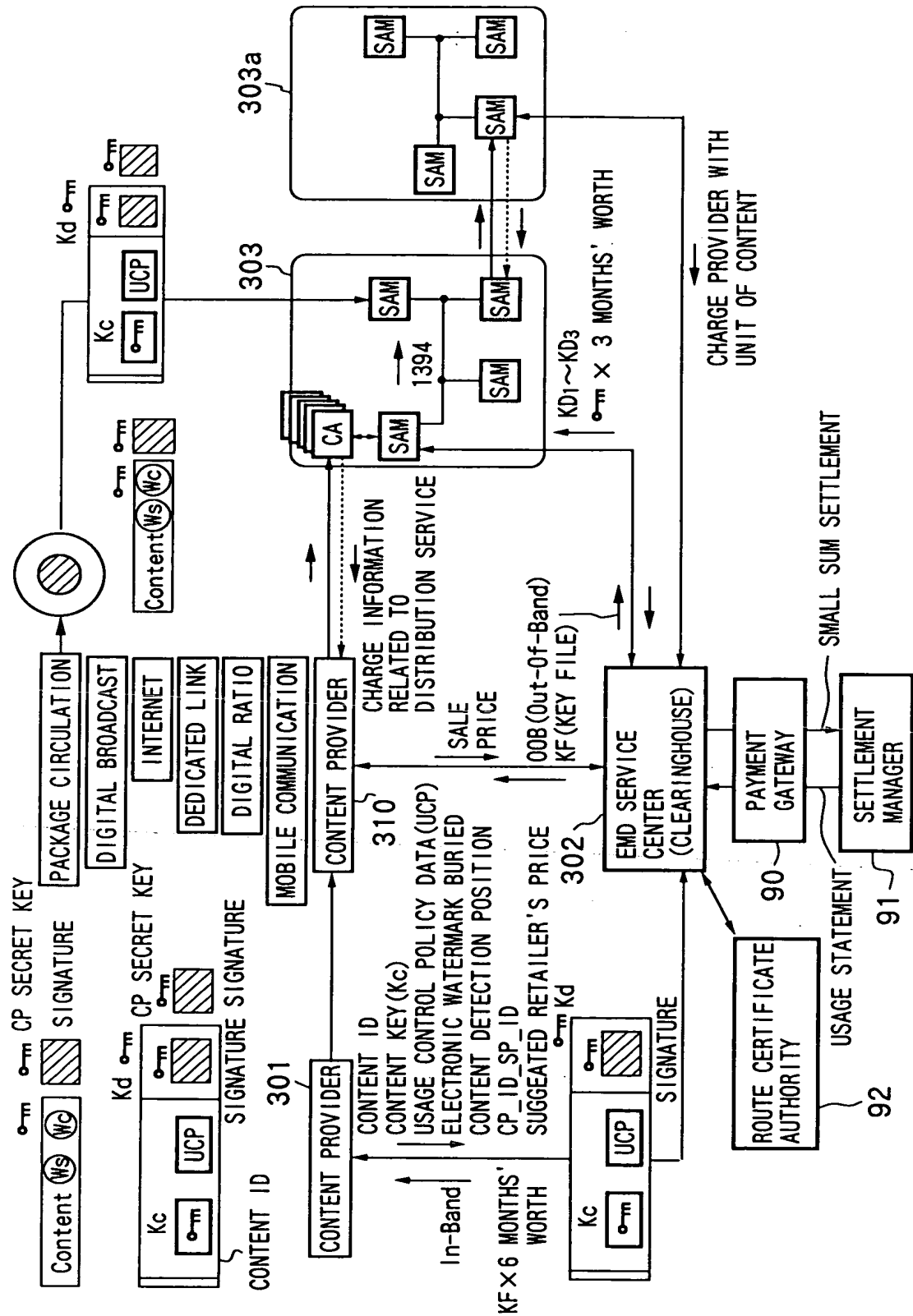


FIG. 86



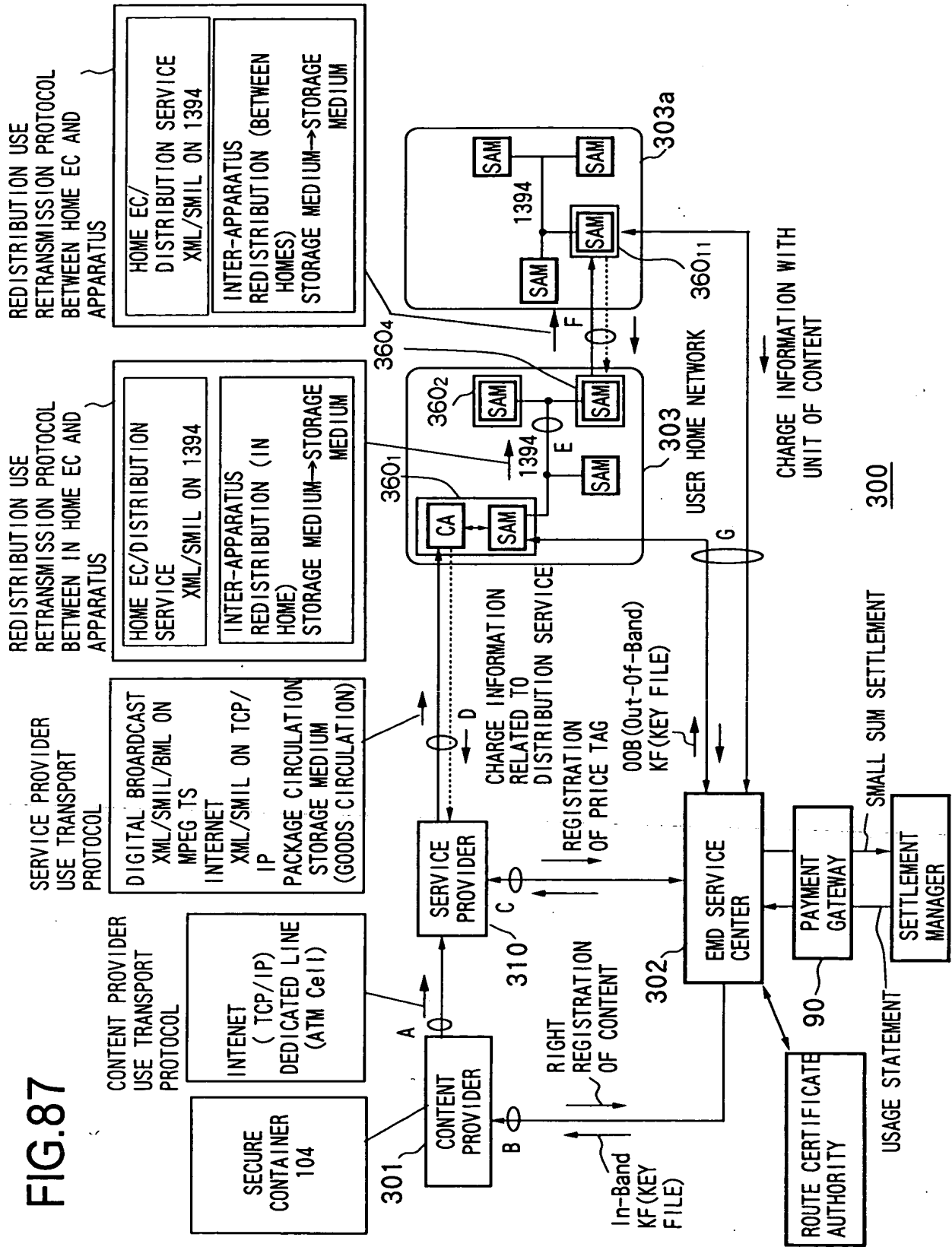


FIG. 88

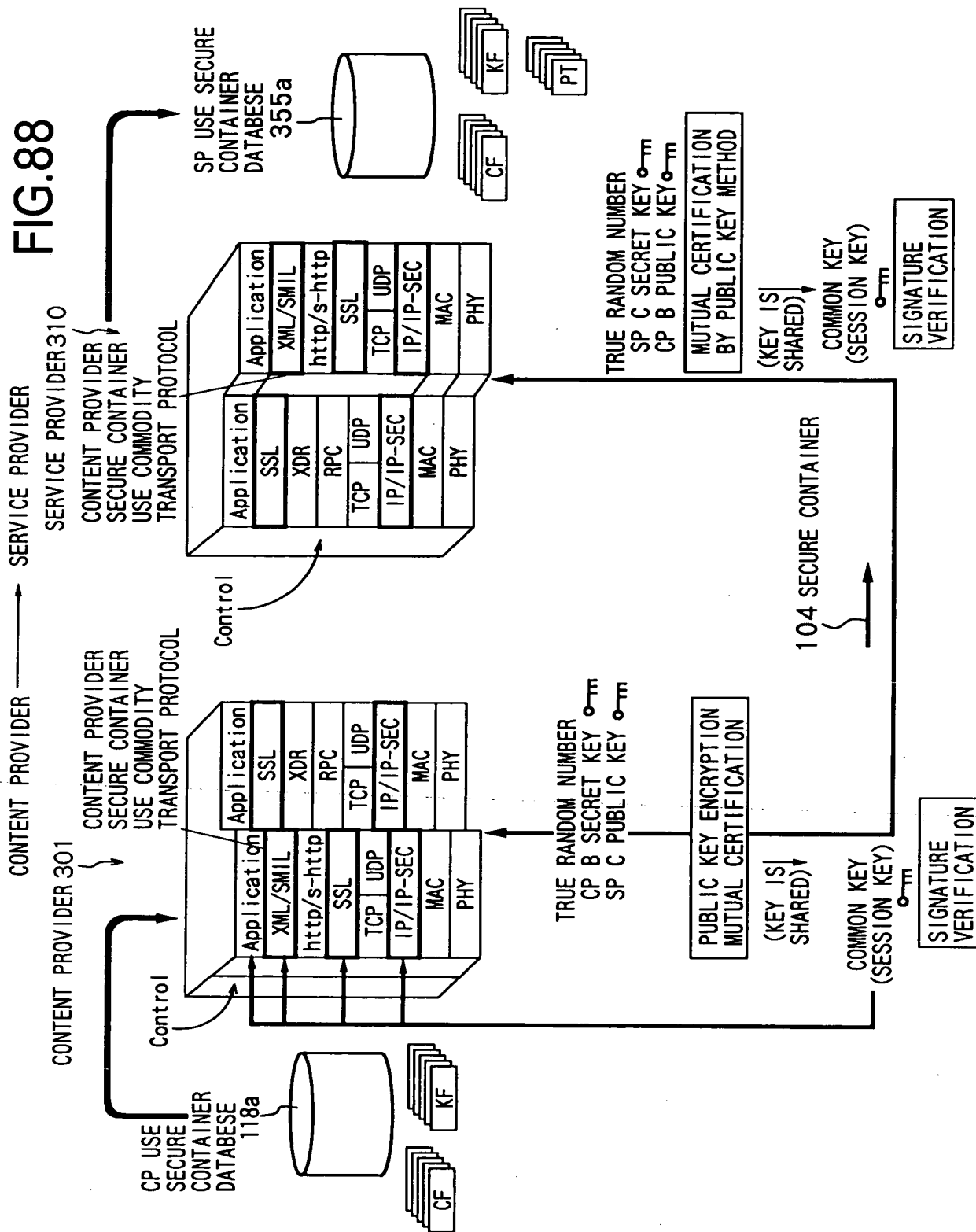


FIG.89

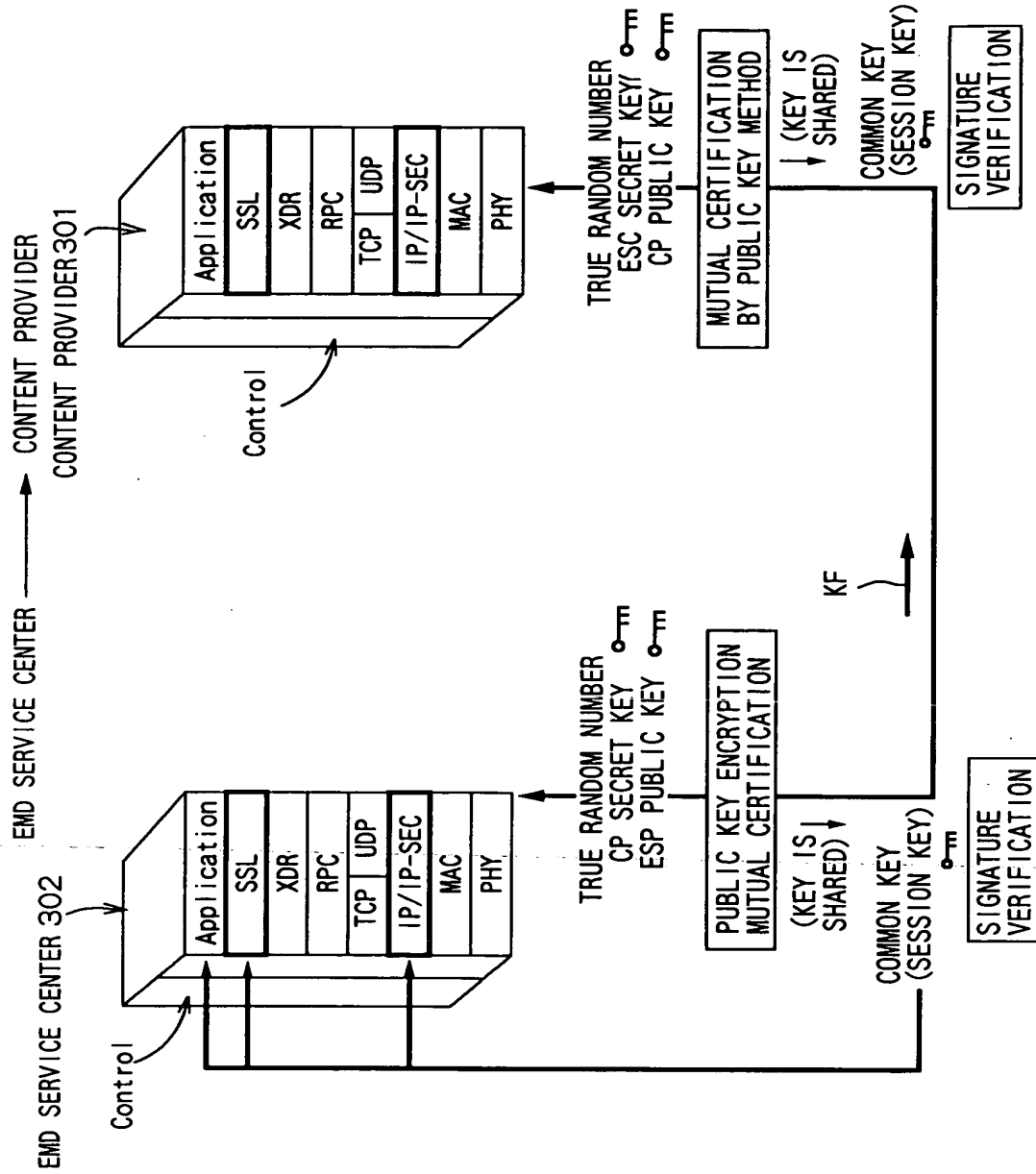


FIG. 90

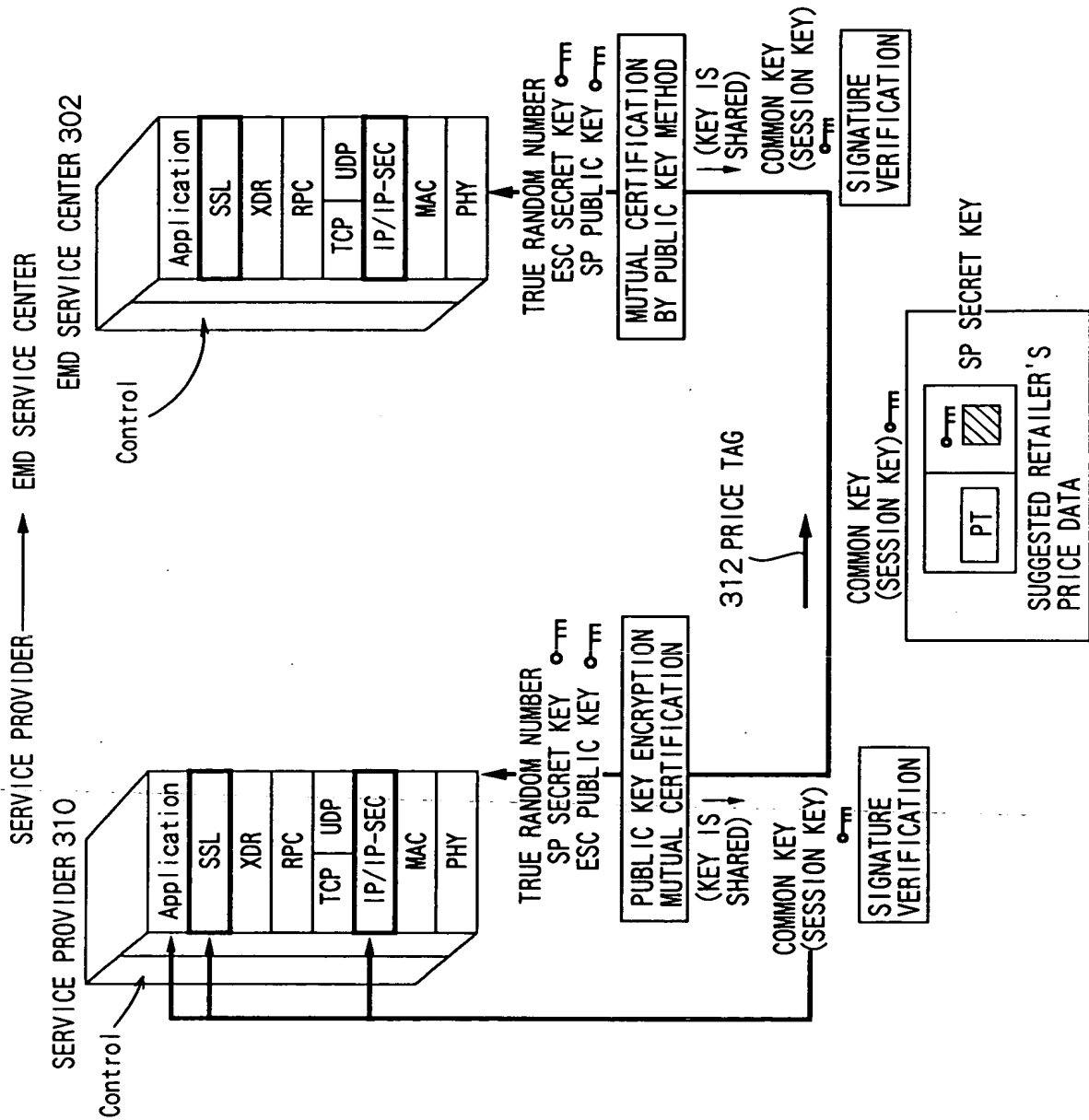


FIG. 91

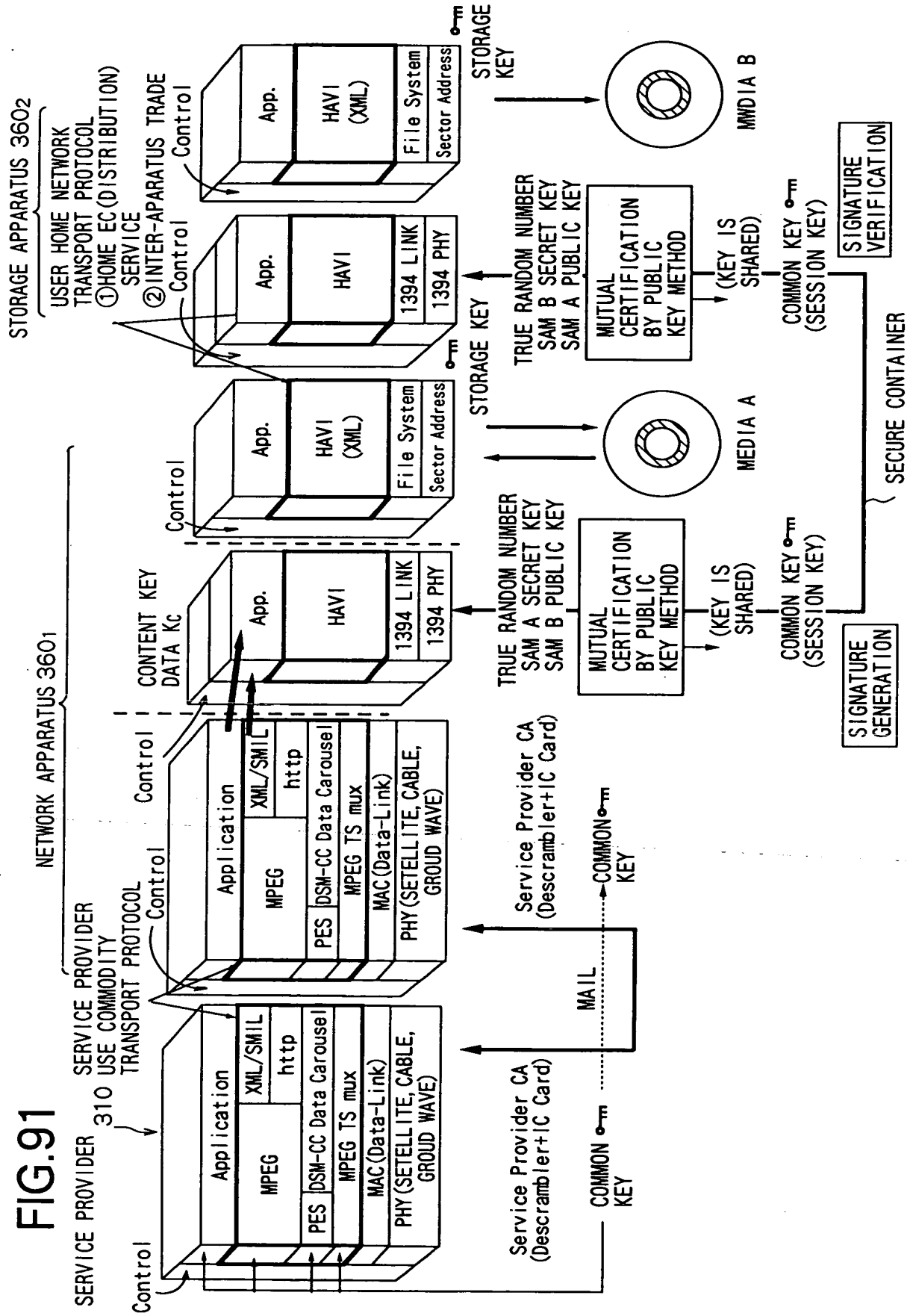


FIG.92

INCREMENT OF SECURE CONTAINER TO PROTOCOL CLASS WHERE
XML/SMIL/BML IS USED IN DATA BROADCAST METHOD OF DIGITAL BROADCAST

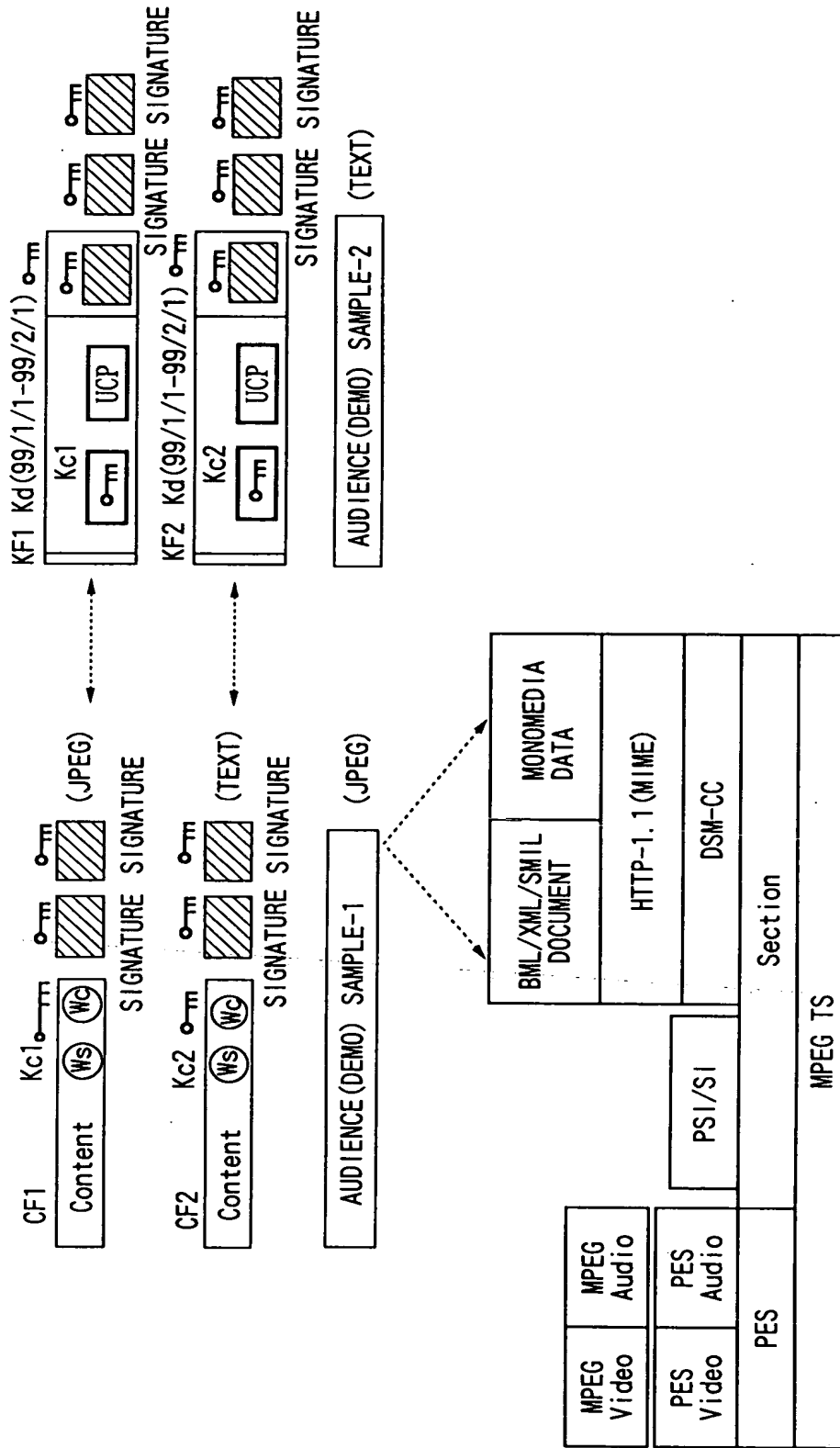


FIG.93

INCREMENT OF SECURE CONTAINER TO PROTOCOL CLASS WHERE
MHEG IS USED IN DATA BROADCAST METHOD OF DIGITAL BROADCAST

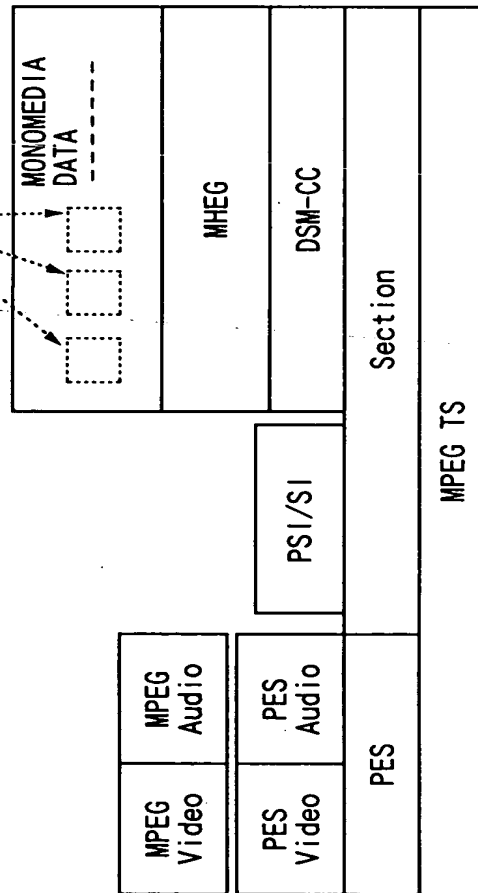
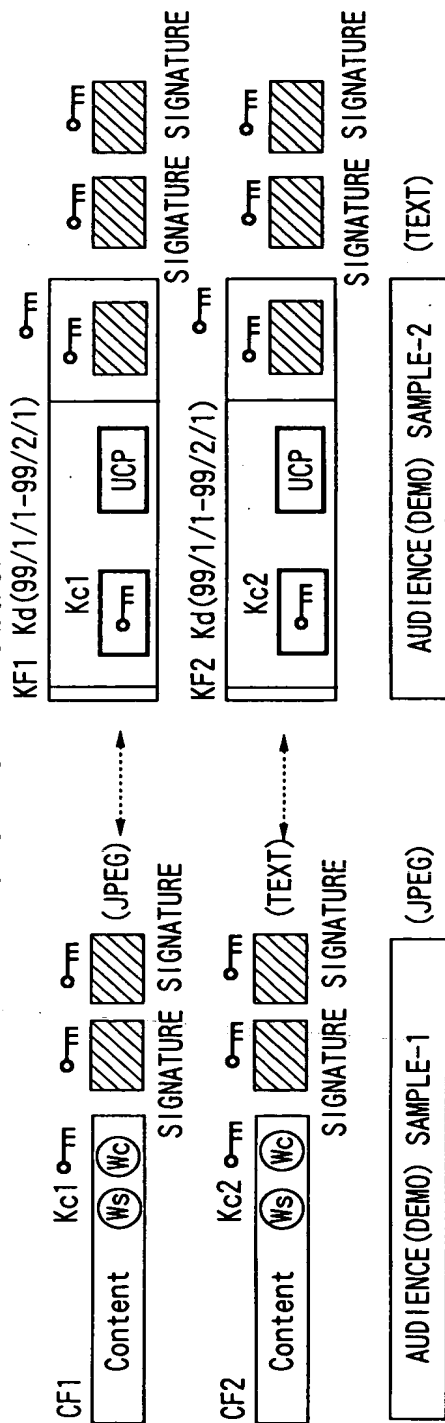


FIG.94

INCREMENT OF SECURE CONTAINER TO PROTOCOL CLASS WHERE
XML/SMIL IS USED IN DATA BROADCAST METHOD OF INTERNET

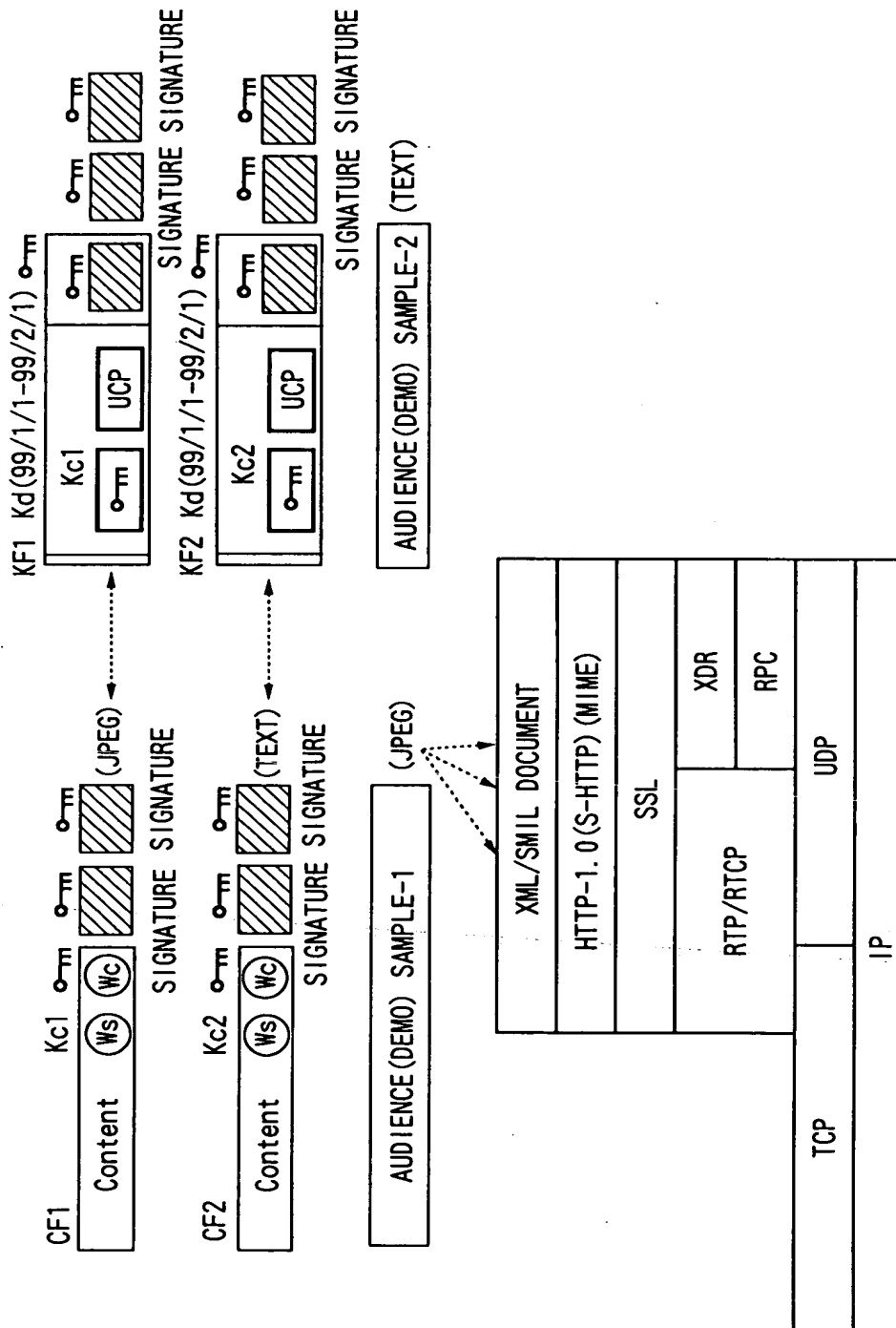


FIG. 95

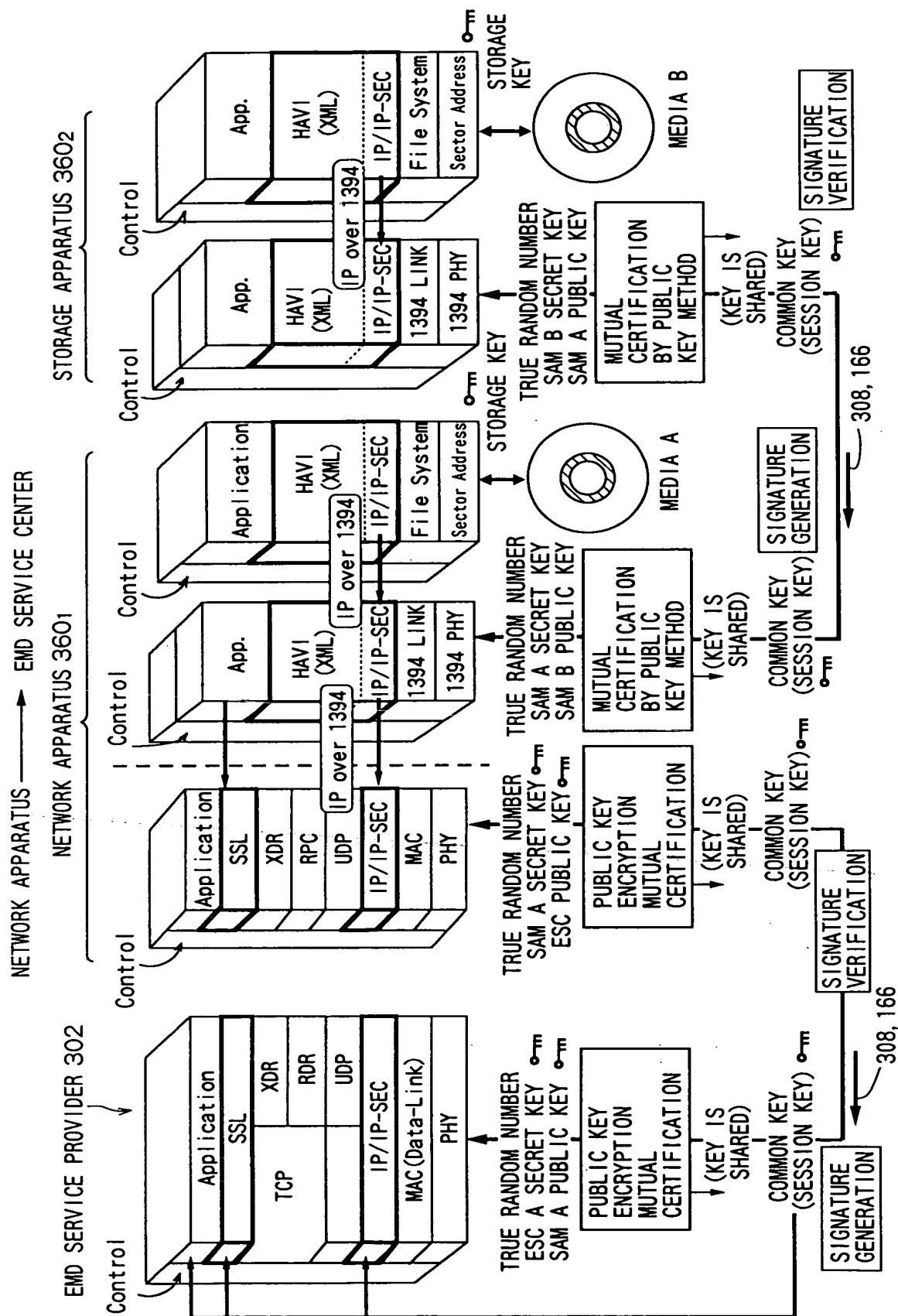


FIG. 96

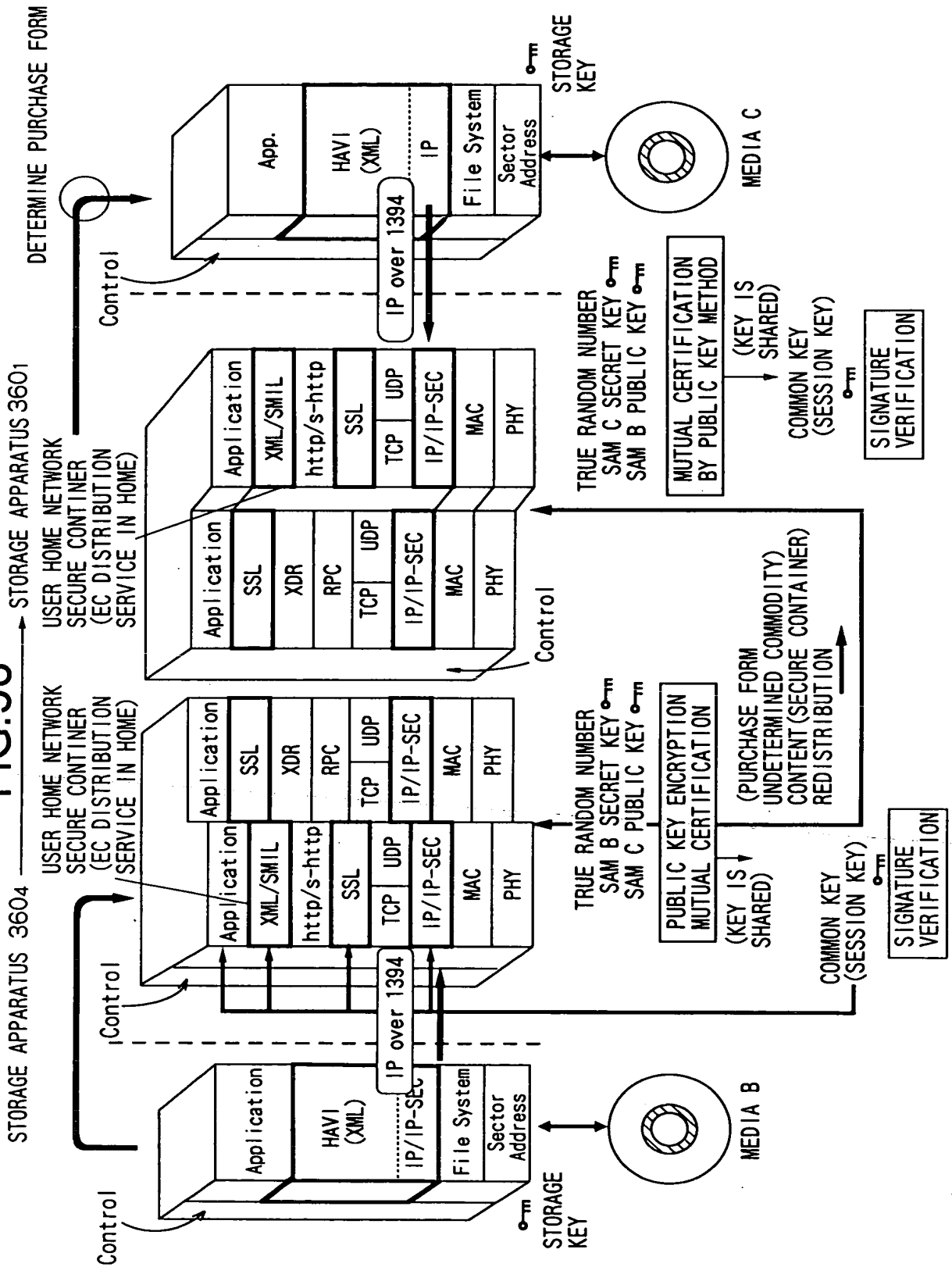
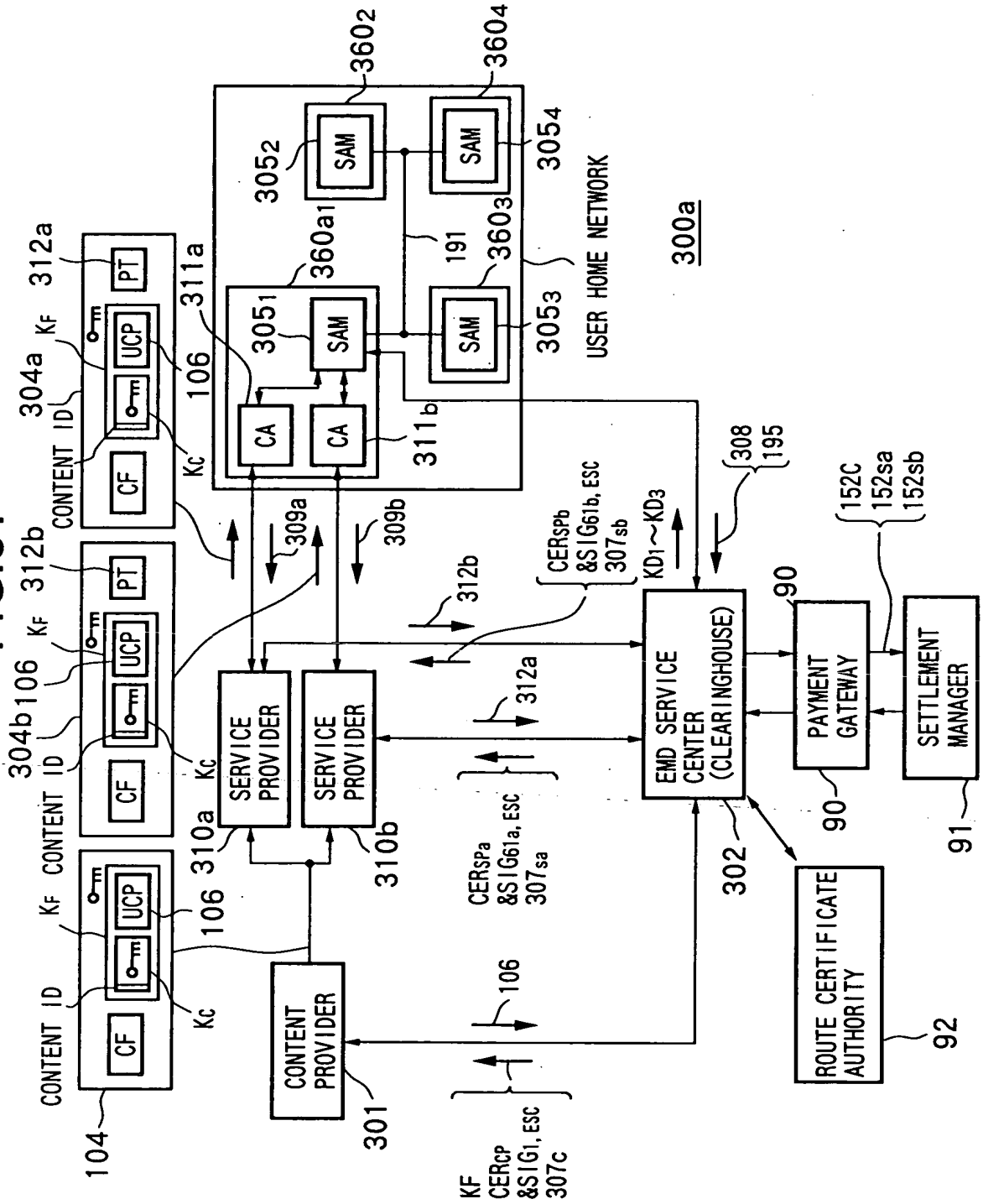


FIG. 97



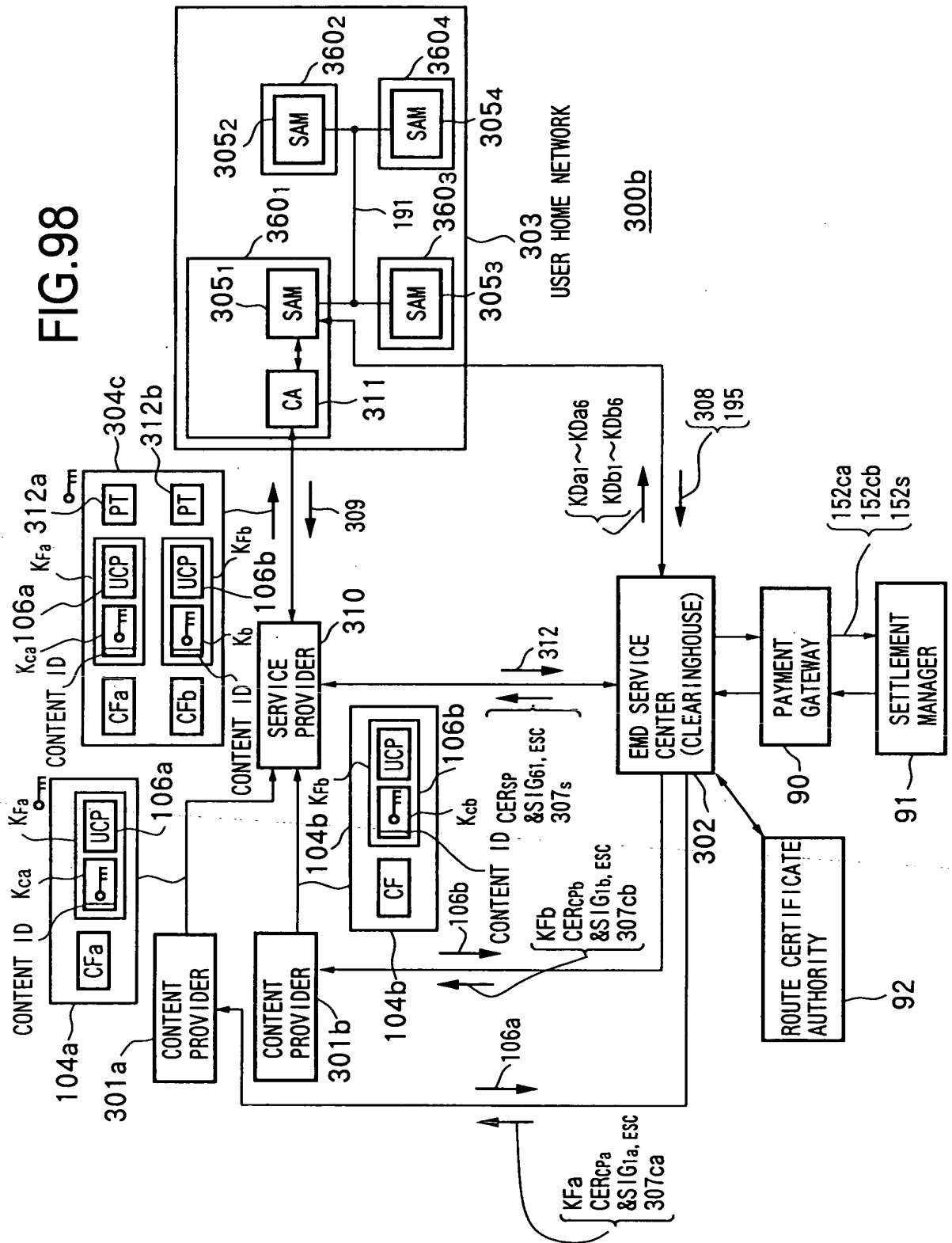


FIG. 99

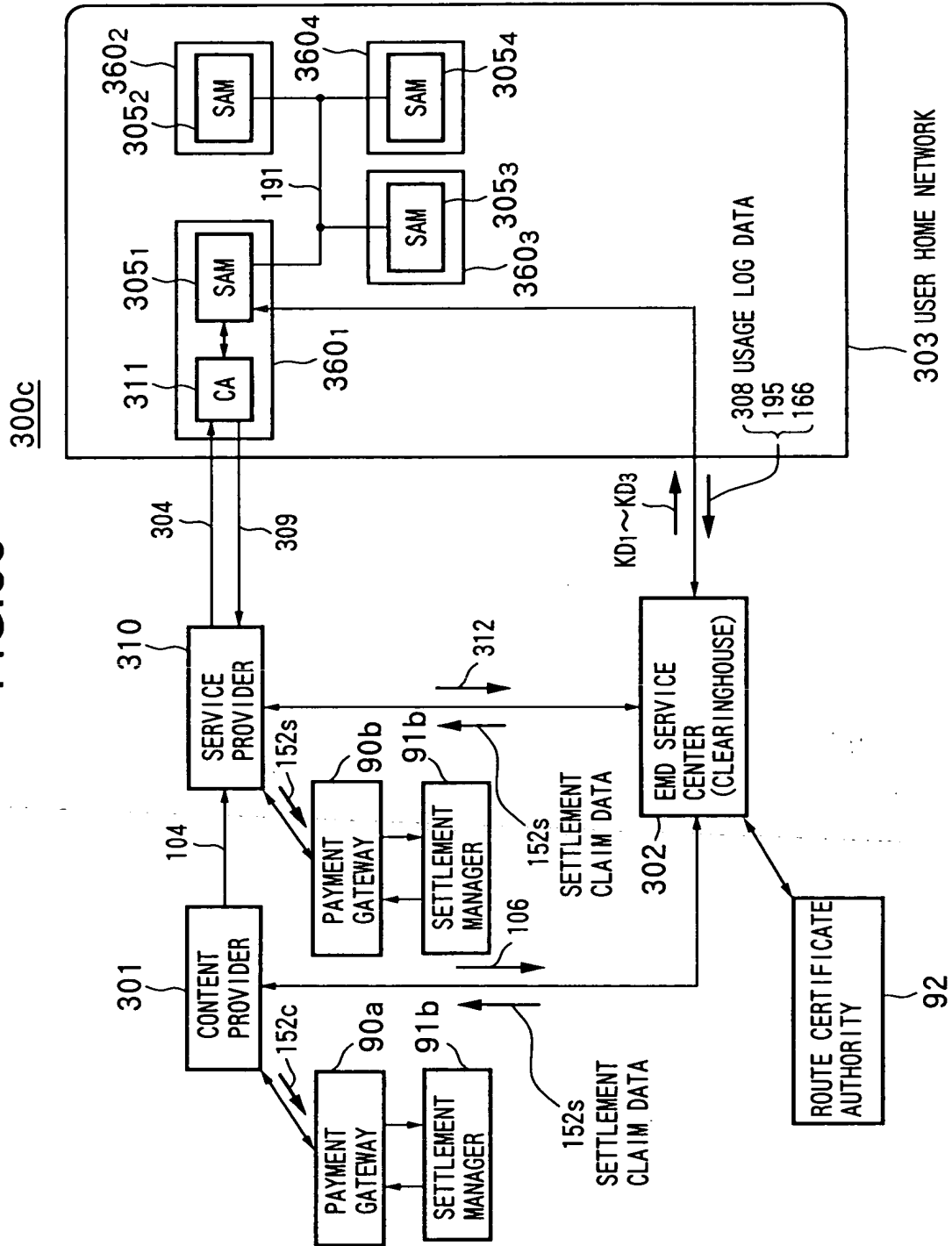


FIG.100

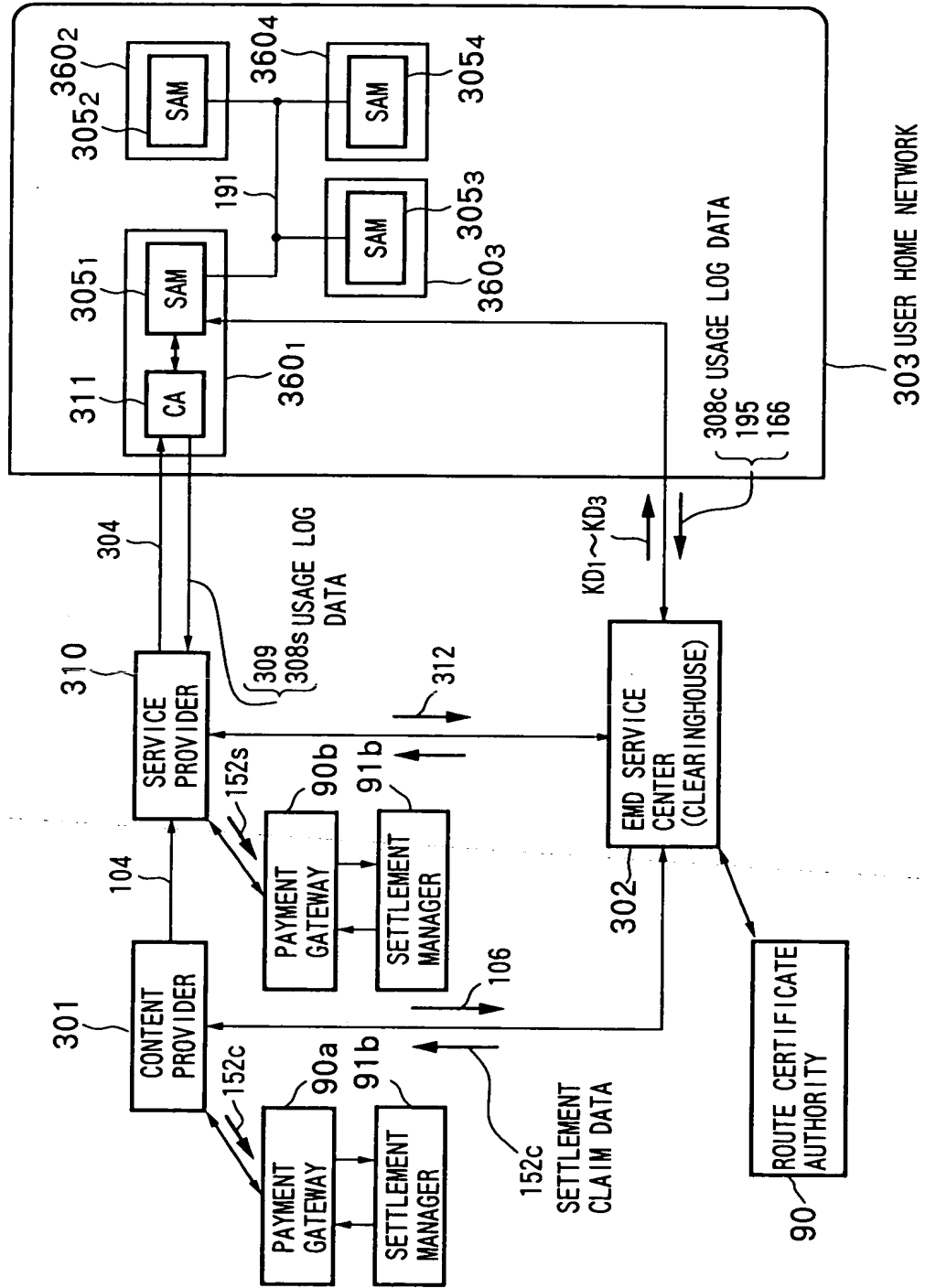
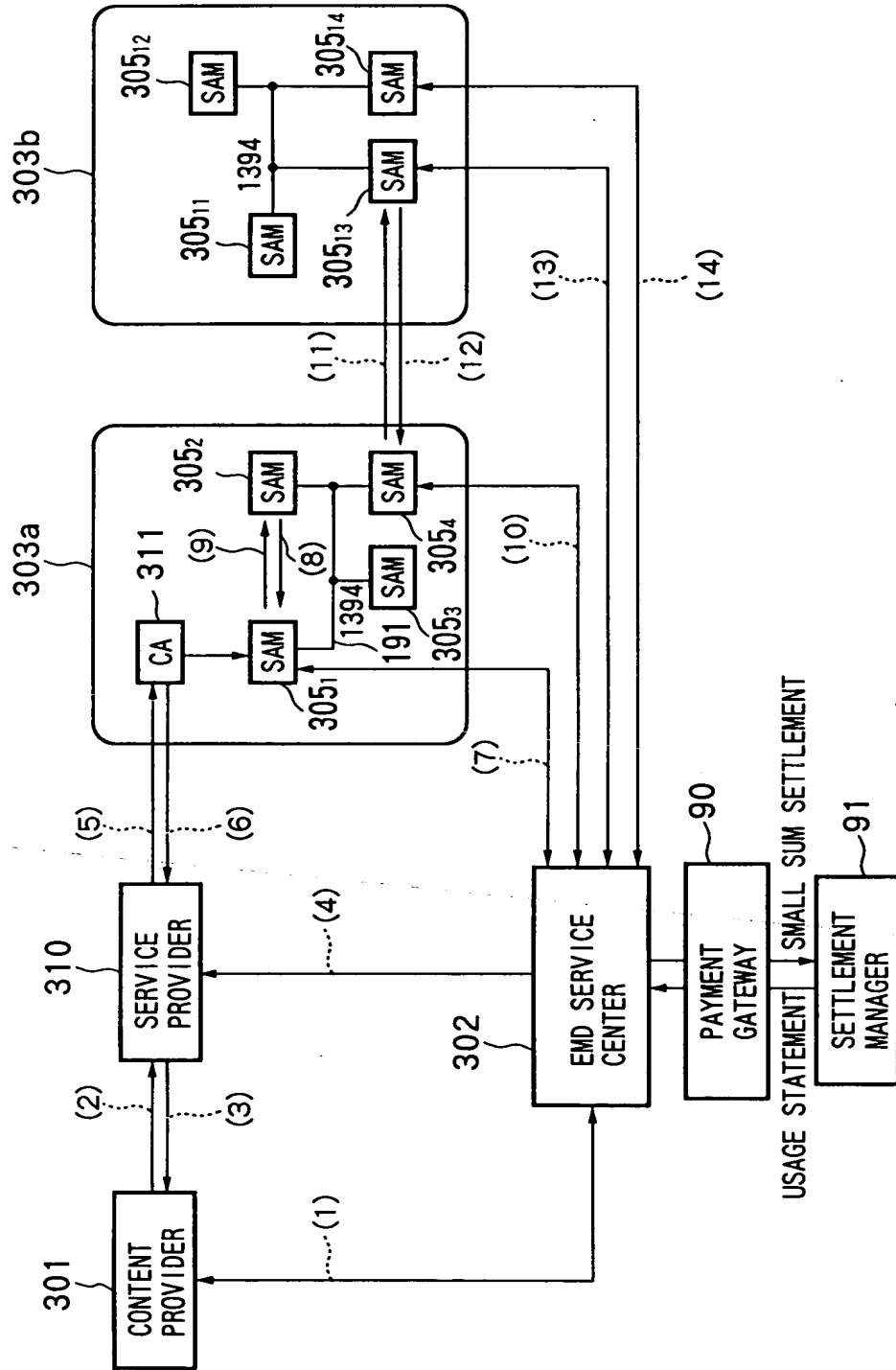


FIG. 101



ACQUISITION ROUTE OF PUBLIC KEY CERTIFICATE

FIG.102

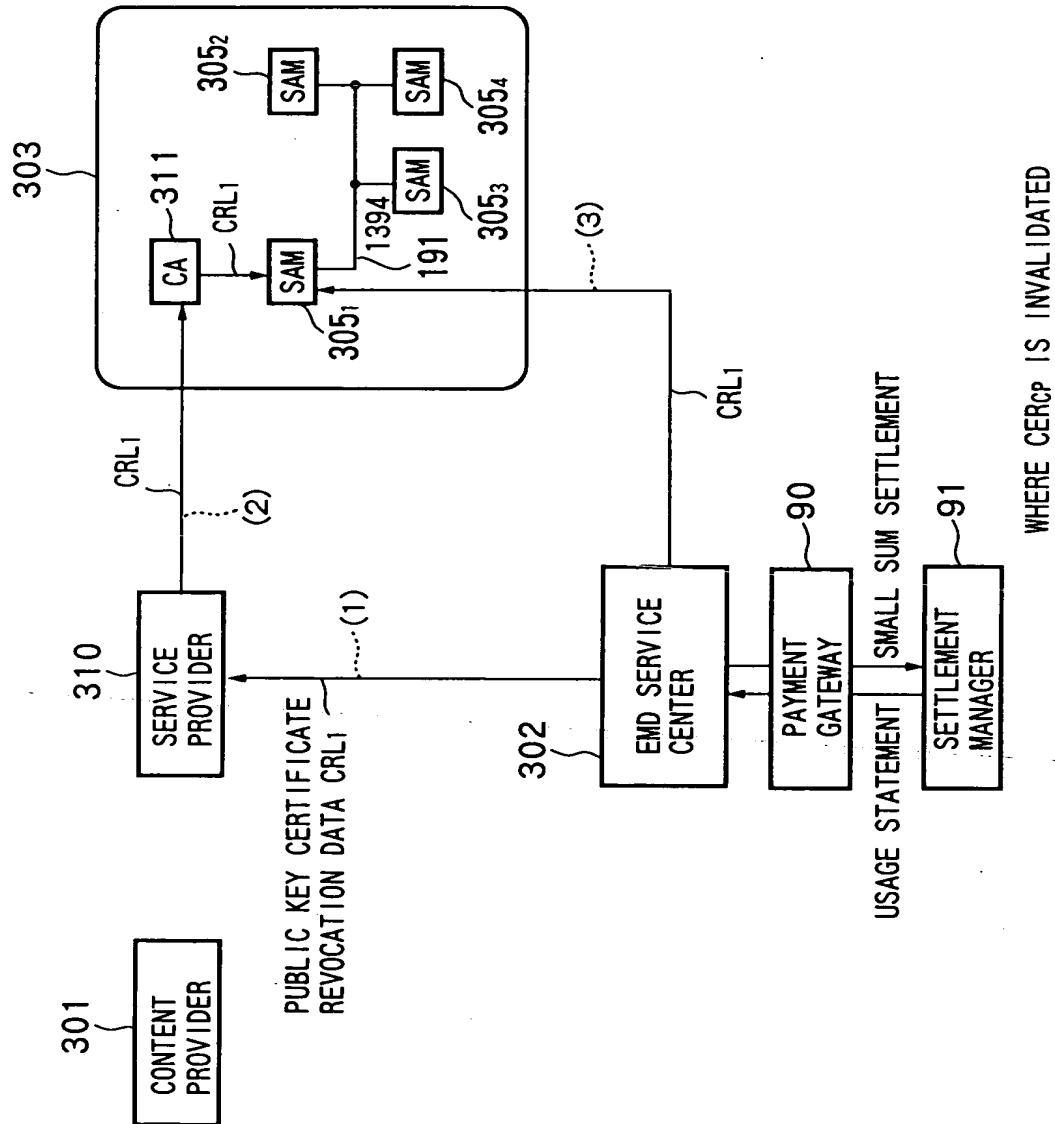
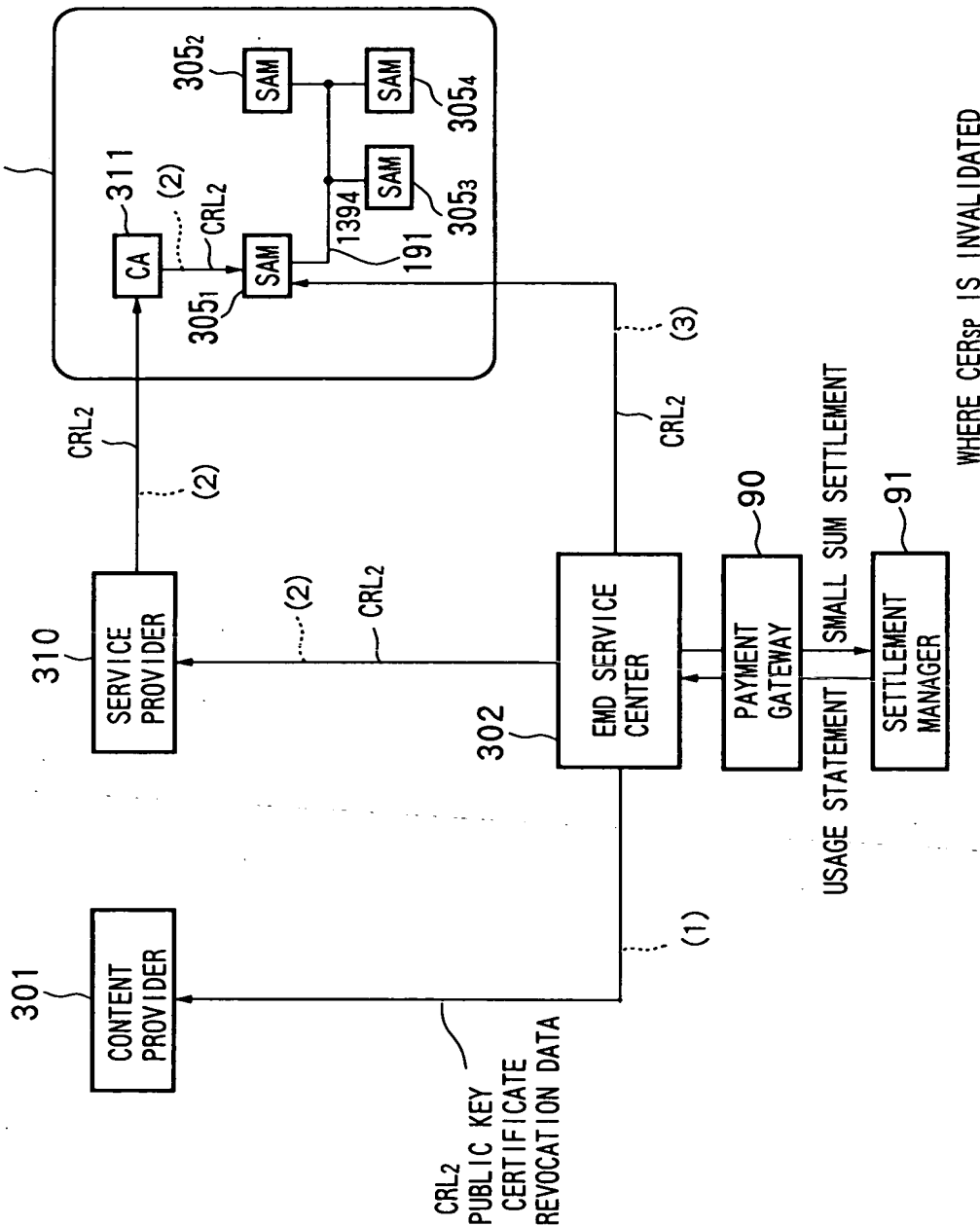
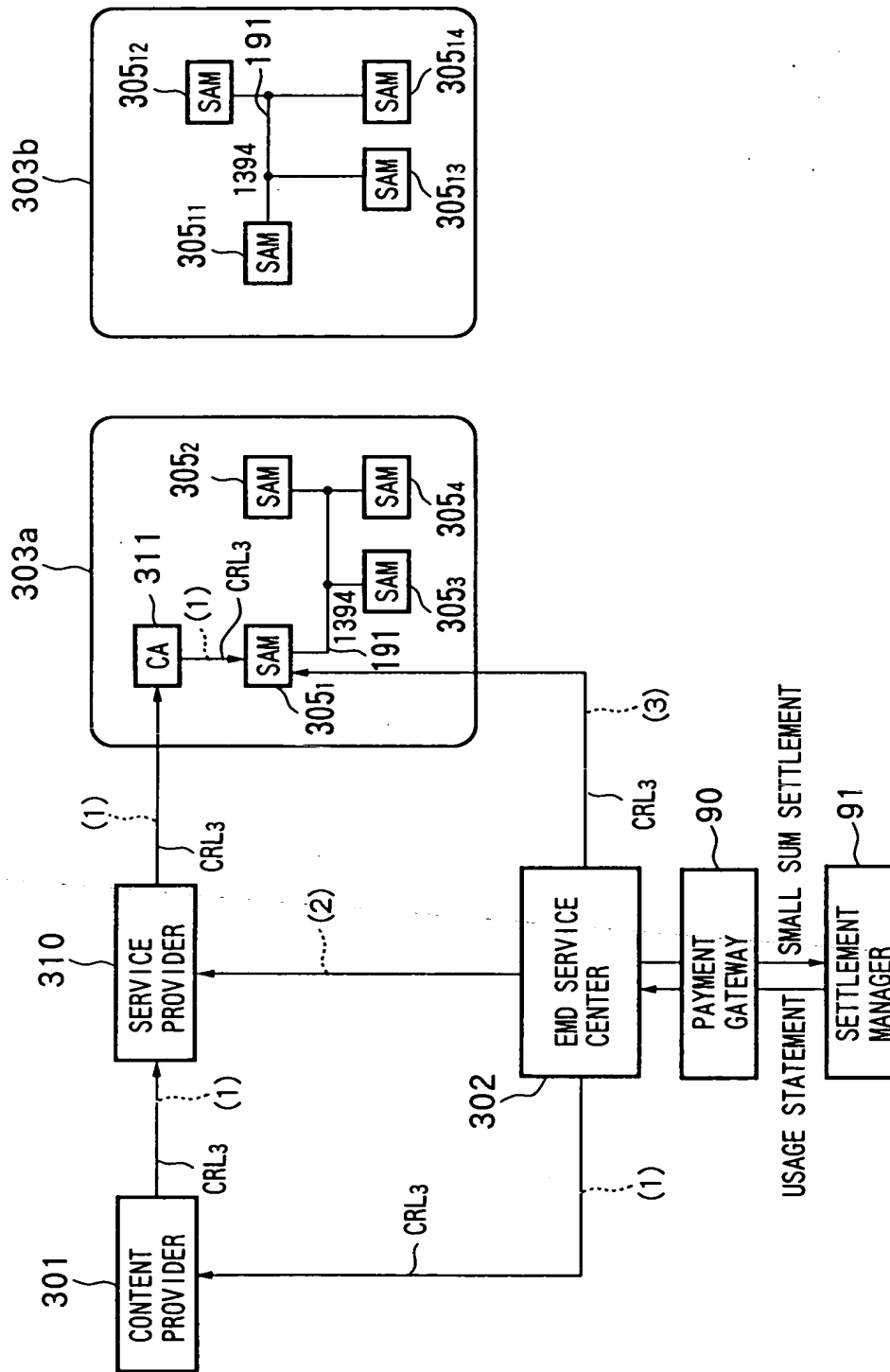


FIG. 103



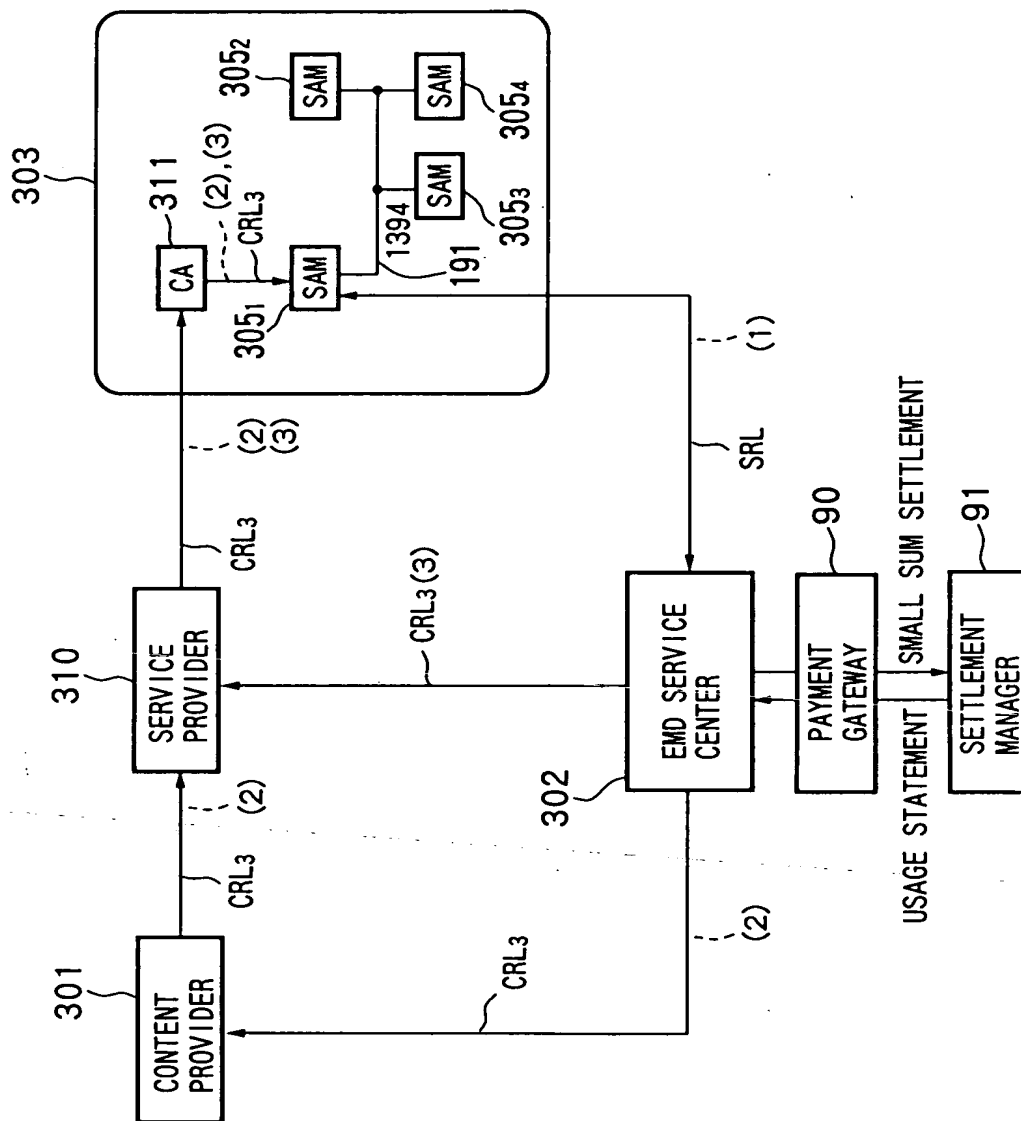
WHERE CERSP IS INVALIDATED

FIG. 104



WHERE CERSAM2 IS INVALIDATED

FIG.105



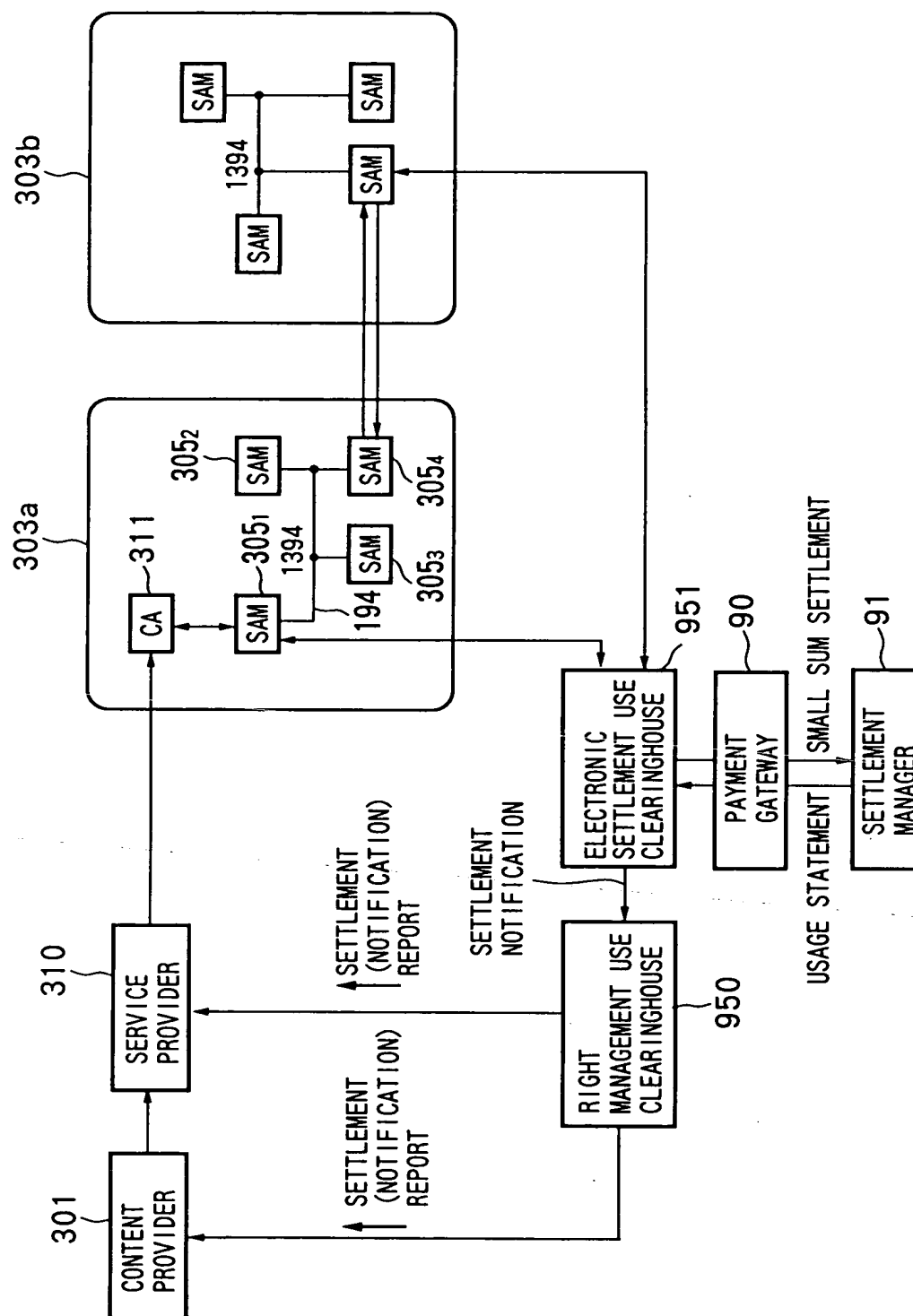


FIG.107

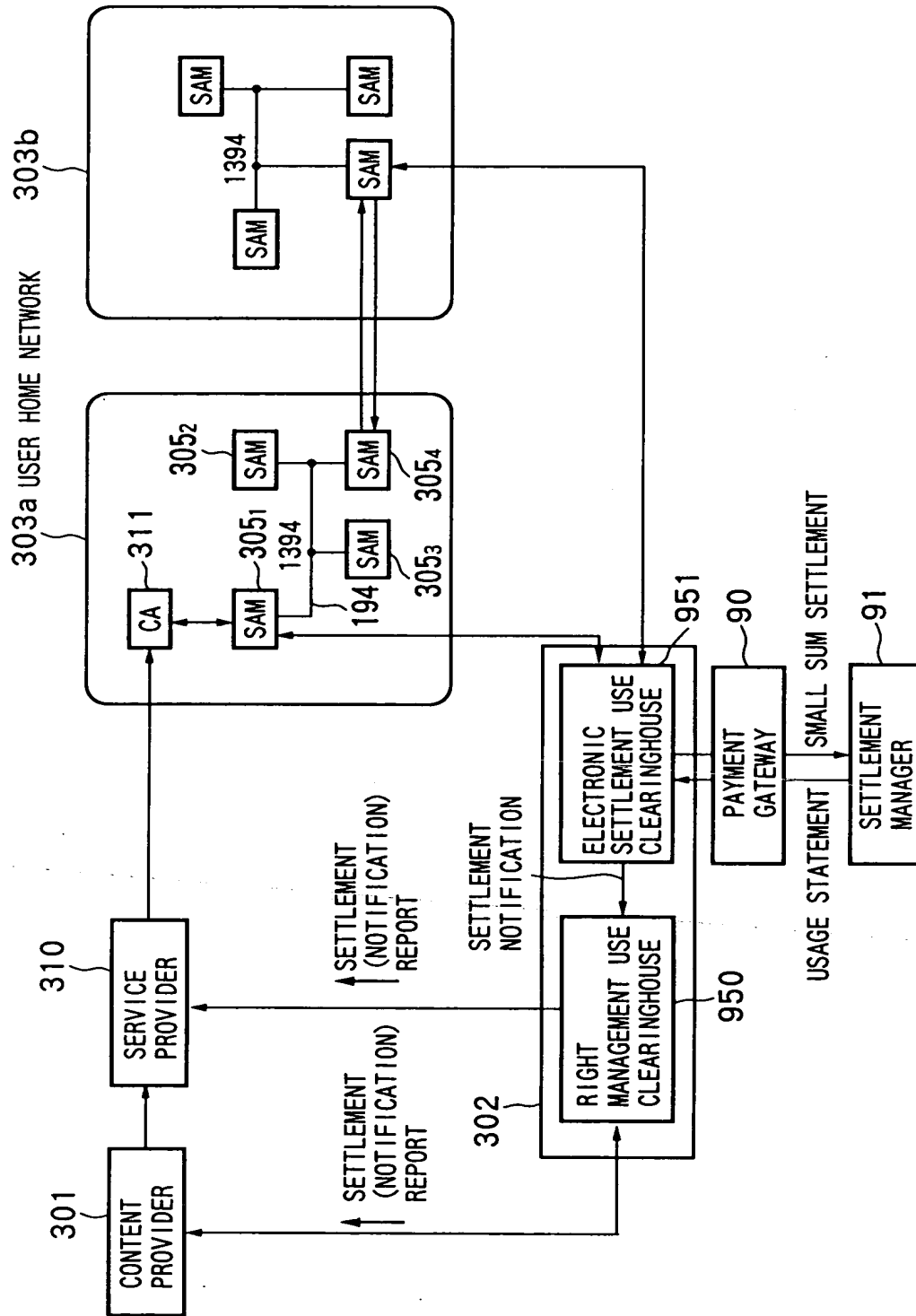


FIG.108

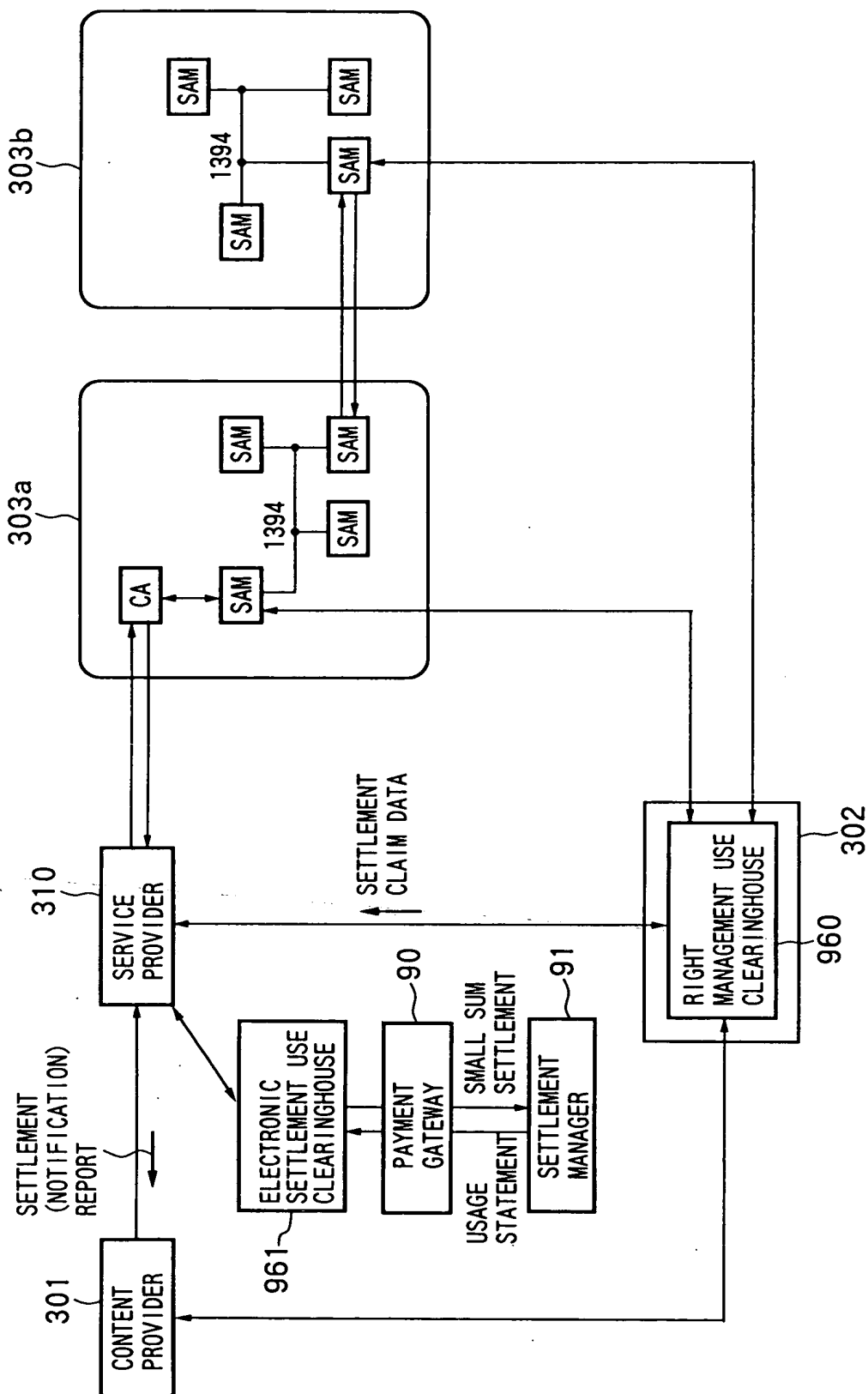
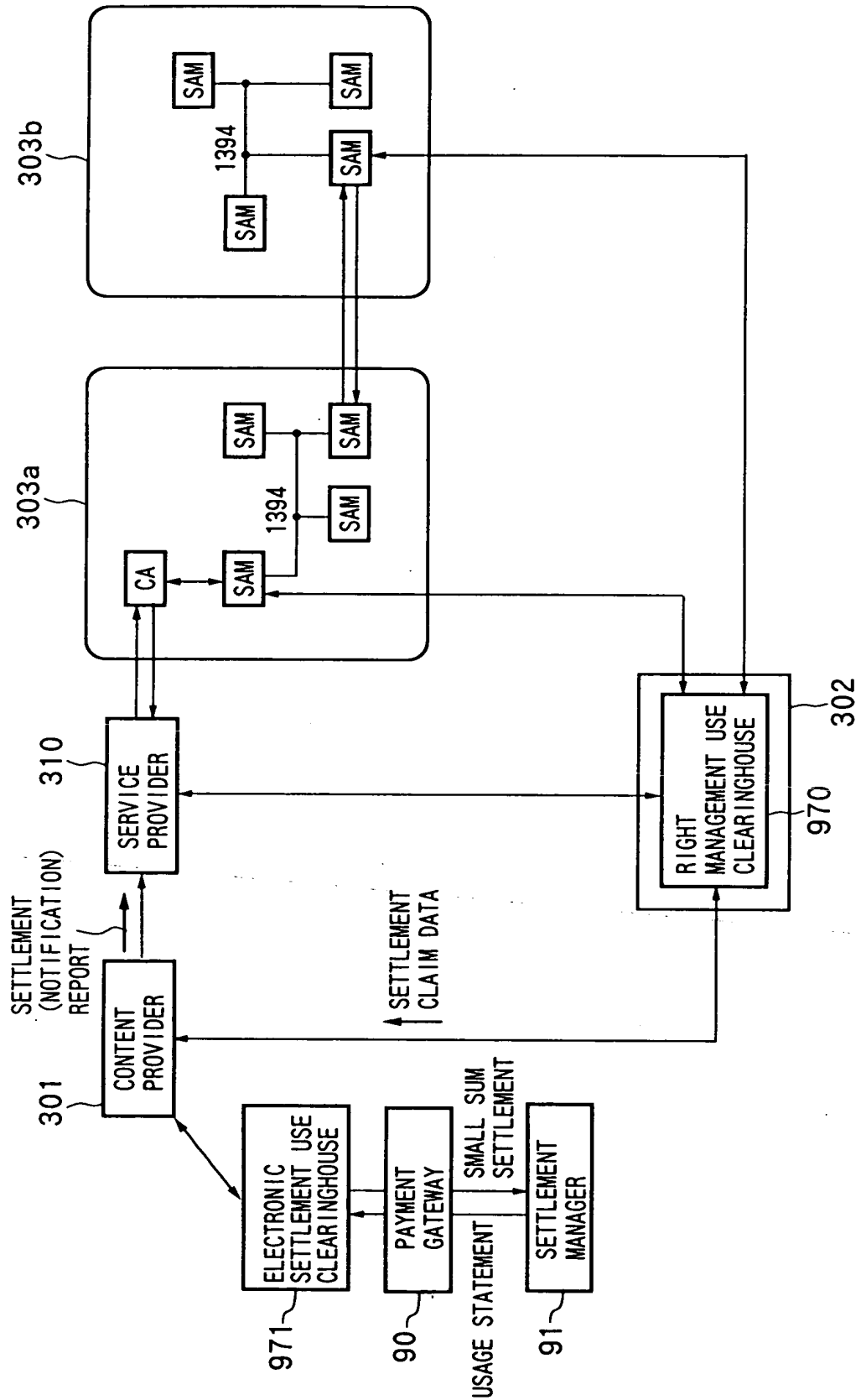


FIG.109



107/143

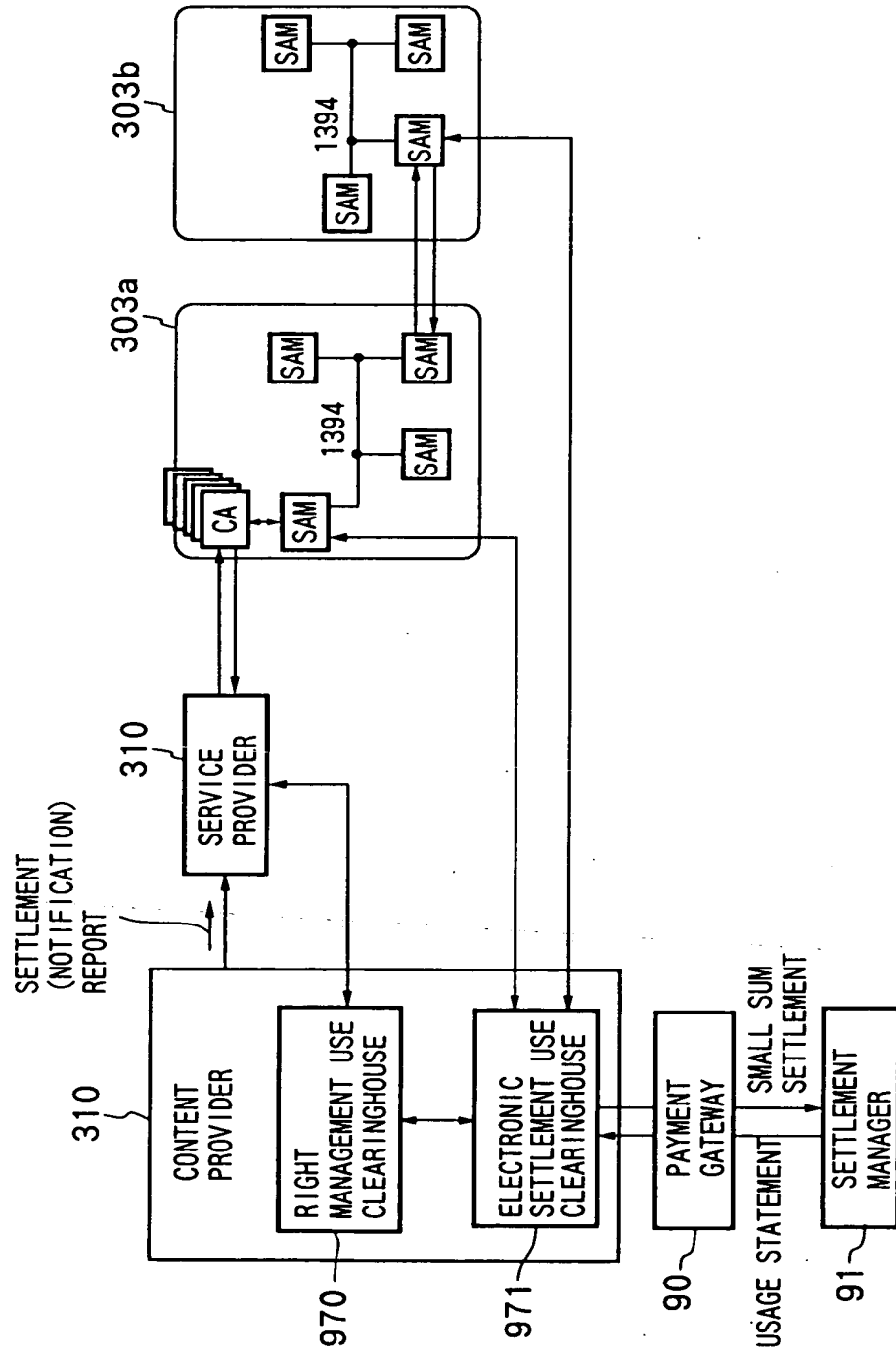


FIG. 111

104a SECURE CONTAINER

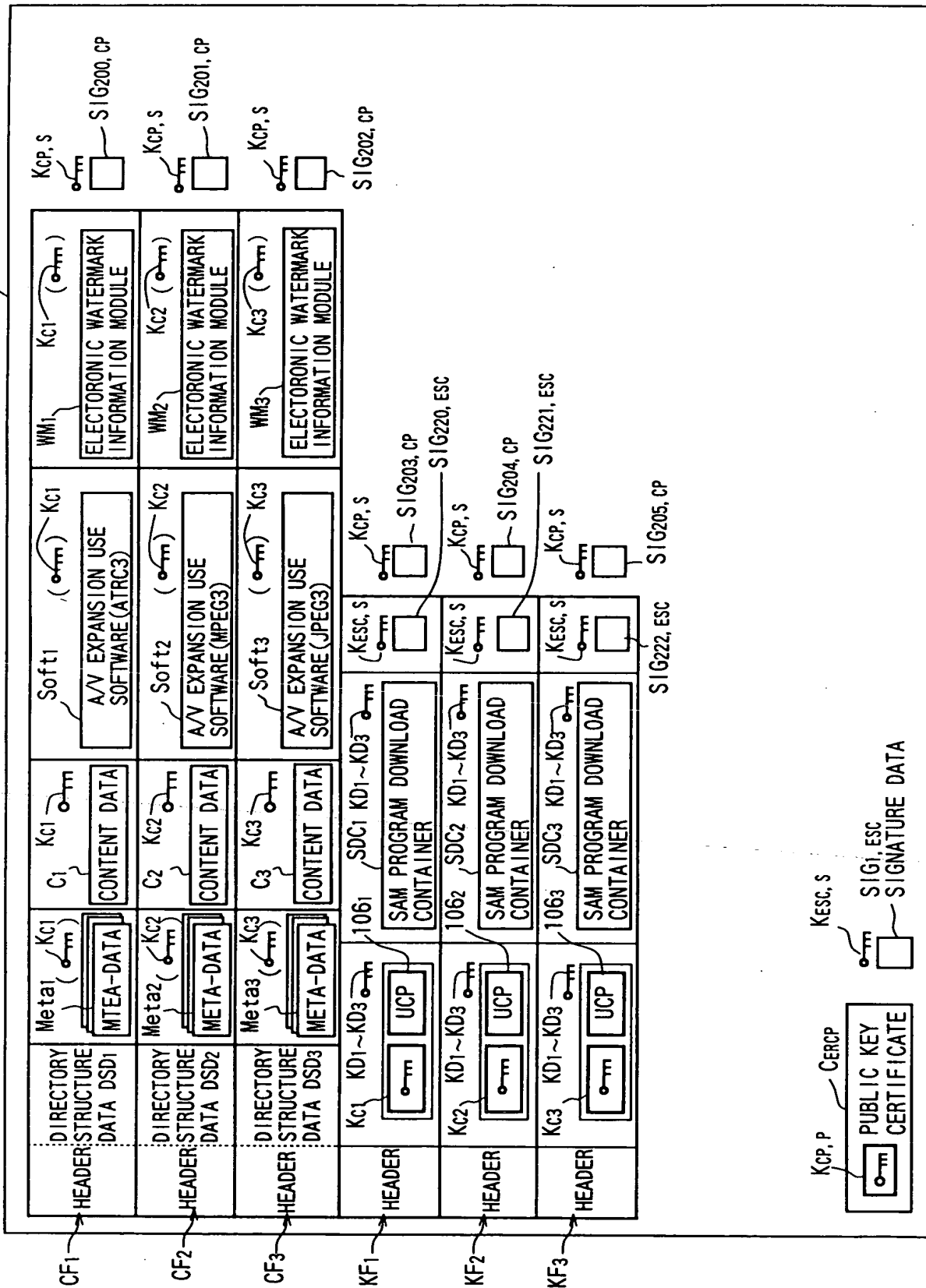


FIG.112

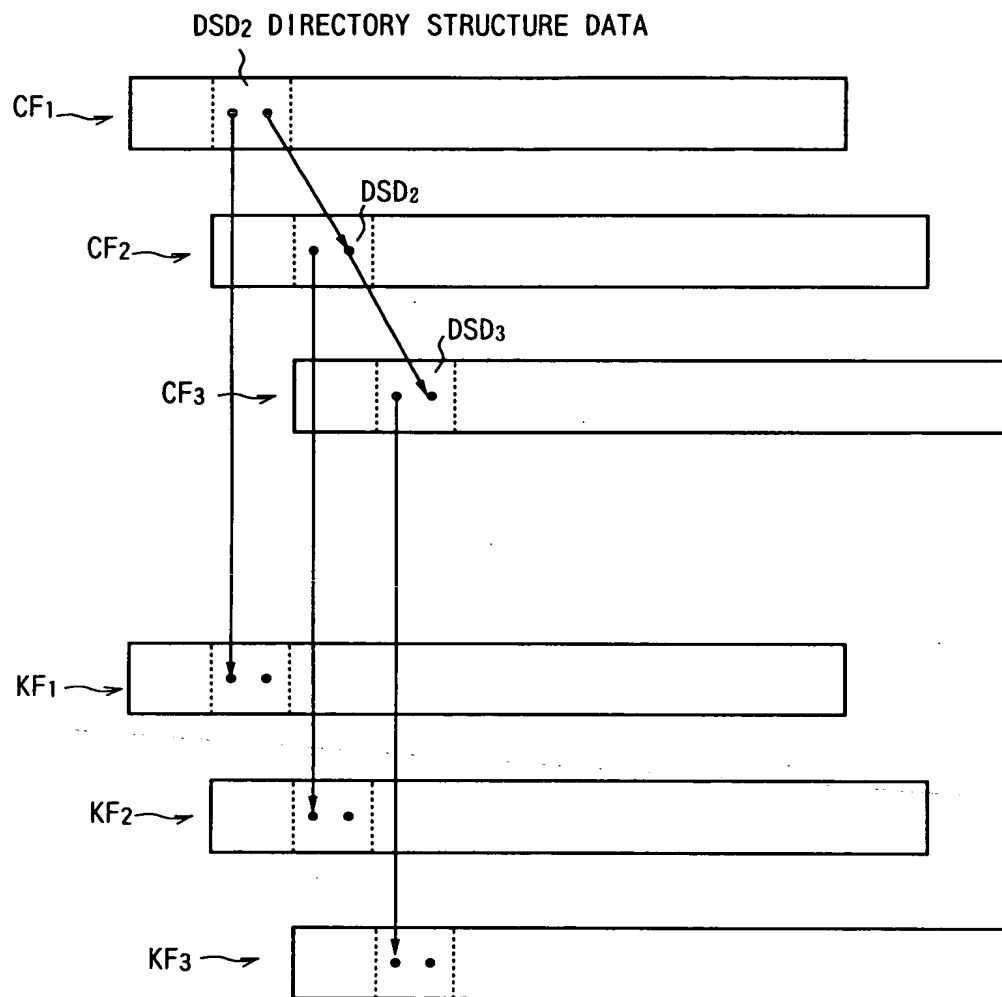


FIG.113

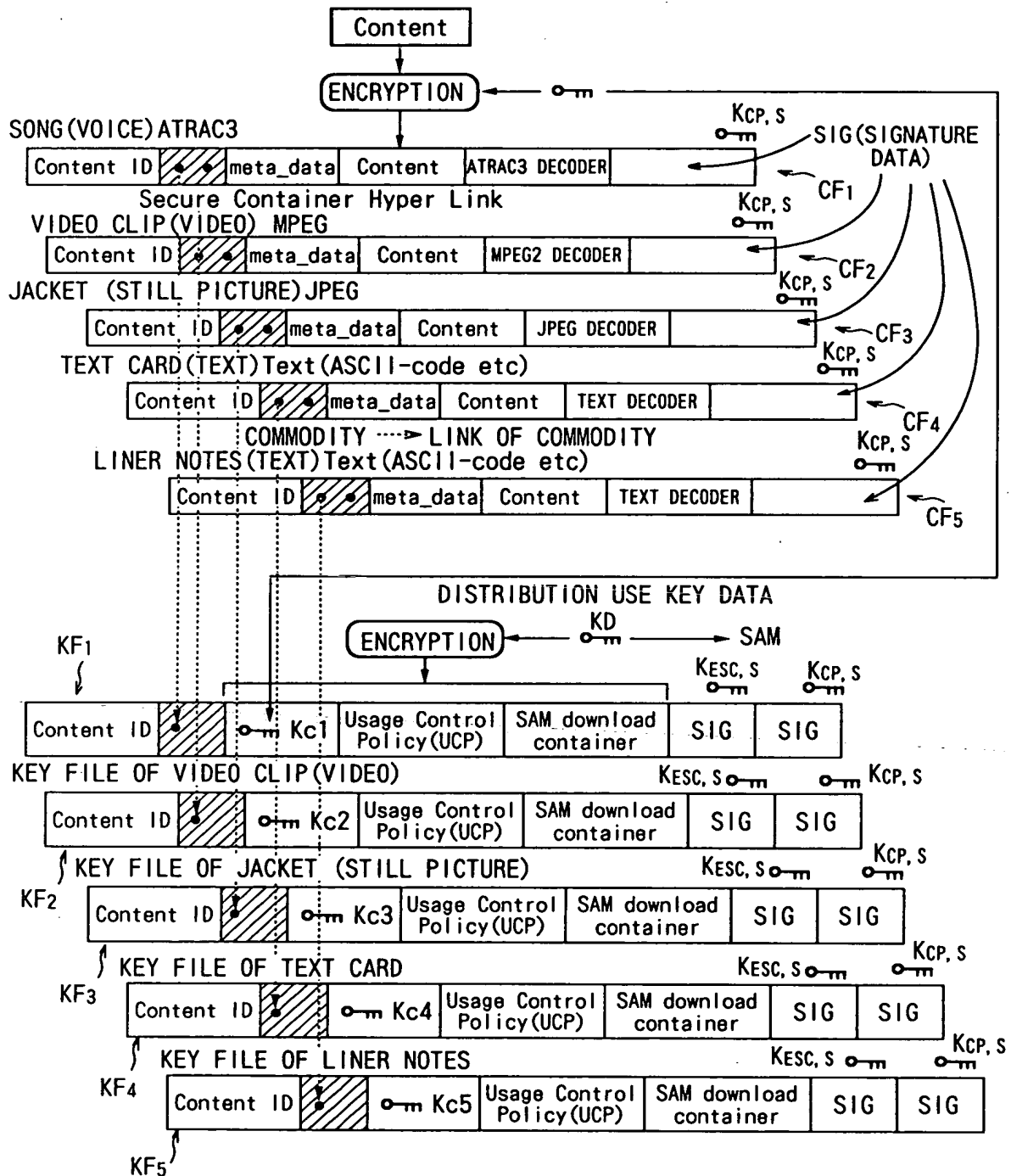


FIG. 114

304a SECURE CONTAINER

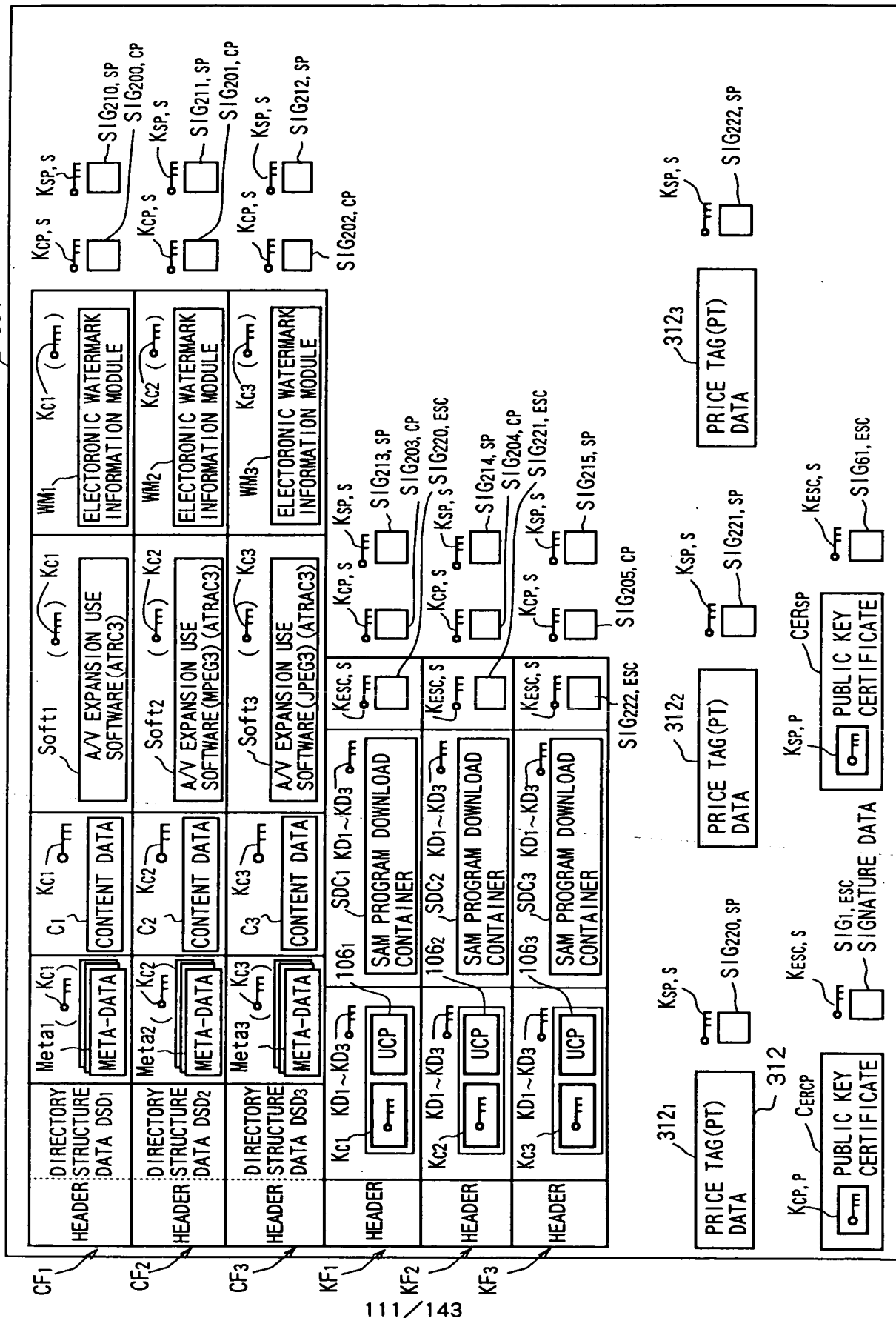


FIG.115

DATA FORMAT OF SECURE CONTAINER (COMPOSITE TYPE)-①

BASIC STRUCTURE

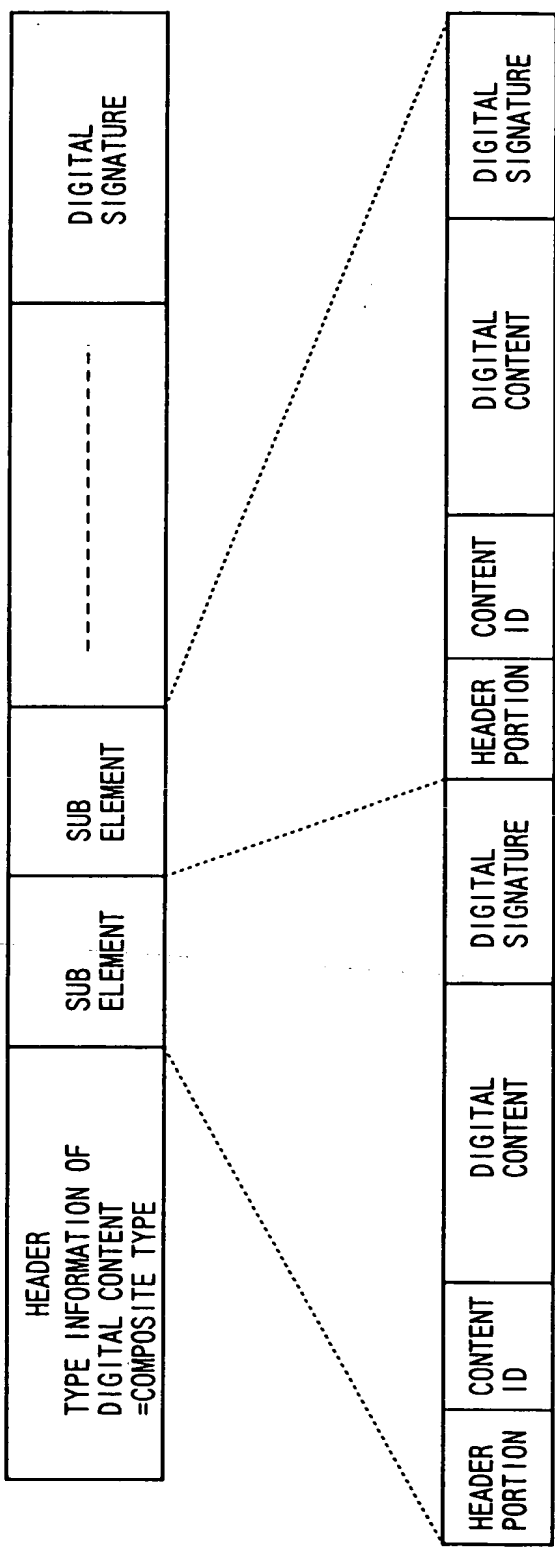
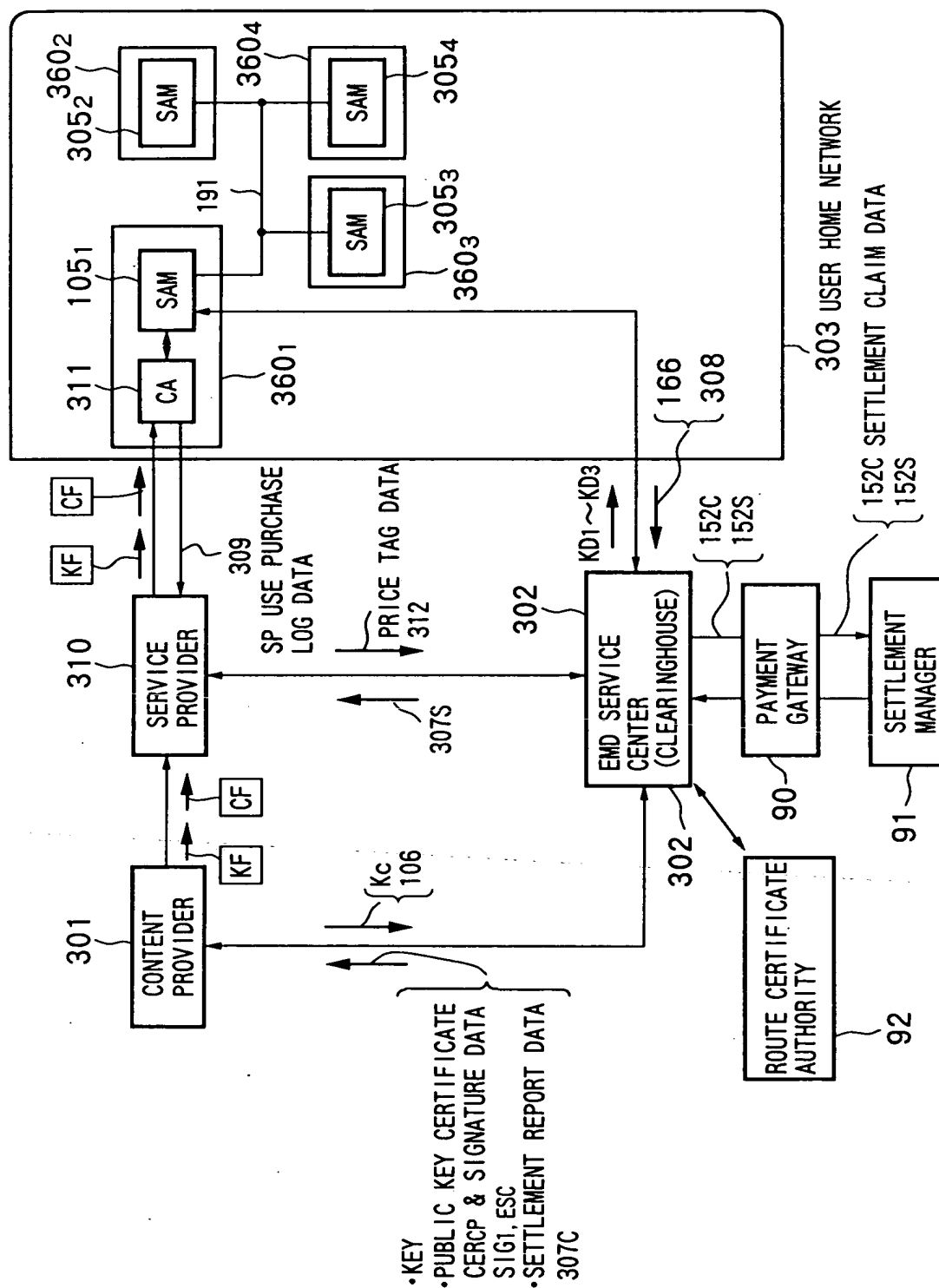


FIG.116

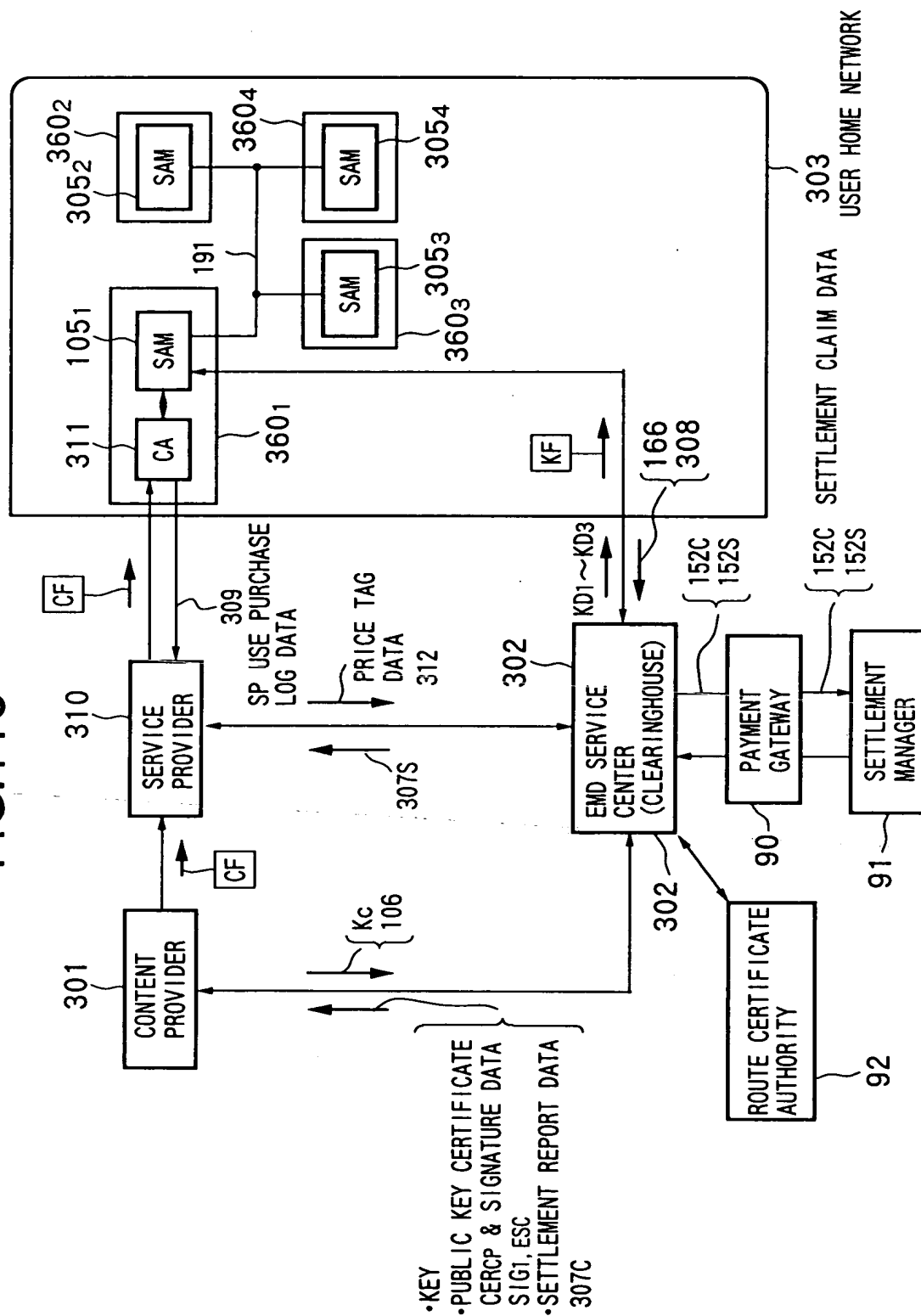
DATA FORMAT OF SECURE CONTAINER (COMPOSITE TYPE) - ②

HEADER PORTION ID	CONTENT ID	PRICE INFORMATION	SIGNATURE
HEADER PORTION ID	CONTENT ID	USAGE CONTROL POLICY DATA , ETC.	HEADER PORTION ID
HEADER PORTION ID	CONTENT ID	VOICE DATA (TUNE)	CONTENT ID
HEADER PORTION ID	CONTENT ID	STILL PICTURE DATA (JACKET)	CONTENT ID
SIGNATURE			
		USAGE CONTROL POLICY DATA , ETC.	SIGNATURE
		VIDEO DATA (VIDEO CLIP)	SIGNATURE
		ALBUM DATA	SIGNATURE

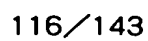
300



300



098676



The diagram illustrates a system architecture for electronic money (EMD) transactions. The components and their interactions are as follows:

- Content Provider (301)**: Interacts with the Service Provider (310) and the EMD Service Center (302).
- Service Provider (310)**: Interacts with the Content Provider (301) and the EMD Service Center (302). It includes a **CF** (Content Fee) component and a **KF** (Key Fee) component.
- EMD Service Center (Clearinghouse) (302)**: The central hub for EMD transactions. It interacts with the Content Provider (301), Service Provider (310), Route Certificate Authority (92), Payment Gateway (90), and Settlement Manager (91). It includes a **KD1~KD3** (Key Data) component.
- Route Certificate Authority (92)**: Provides route certificates to the EMD Service Center.
- Payment Gateway (90)**: Facilitates payments between the EMD Service Center and the Settlement Manager.
- Settlement Manager (91)**: Manages the settlement of transactions, receiving data from the Payment Gateway.
- User Home Network (303)**: A large box representing the user's environment, containing:
 - Settlement Claim Data (308)**: Data used for settling transactions.
 - Settlement Claim Data (309)**: Data used for settling transactions.
 - Price Tag Data (312)**: Data used for pricing transactions.
 - SP Use Purchase Log Data (309)**: Data used for logging purchases.
 - CA (311)**: Certificate Authority component.
 - SAM (3051, 3052, 3053, 3054)**: Secure Account Manager components.
 - KF (3061)**: Key Fee component.

The diagram shows the flow of data and components between these entities, illustrating the system architecture for EMD transactions.

FIG. 121

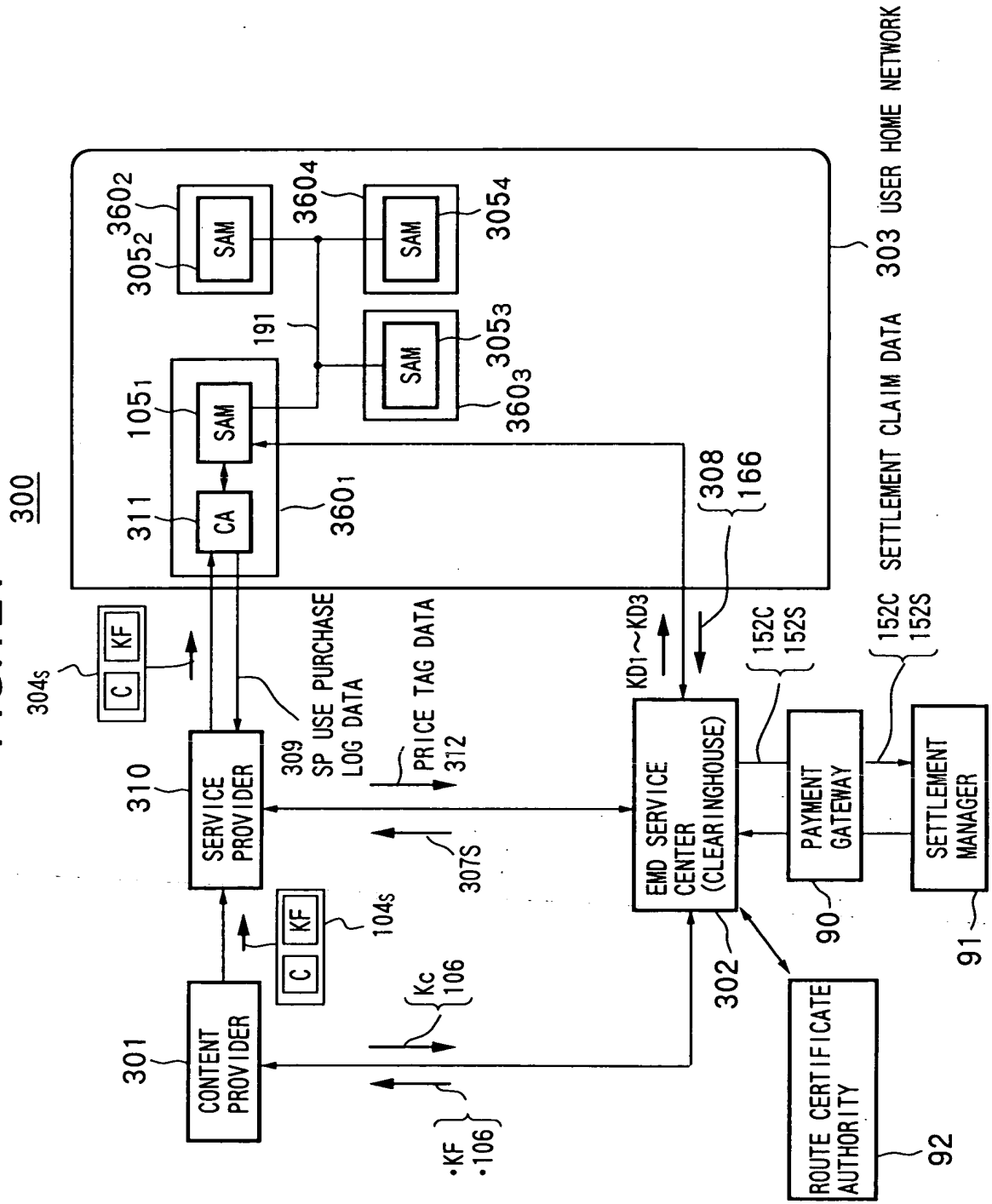


FIG. 122

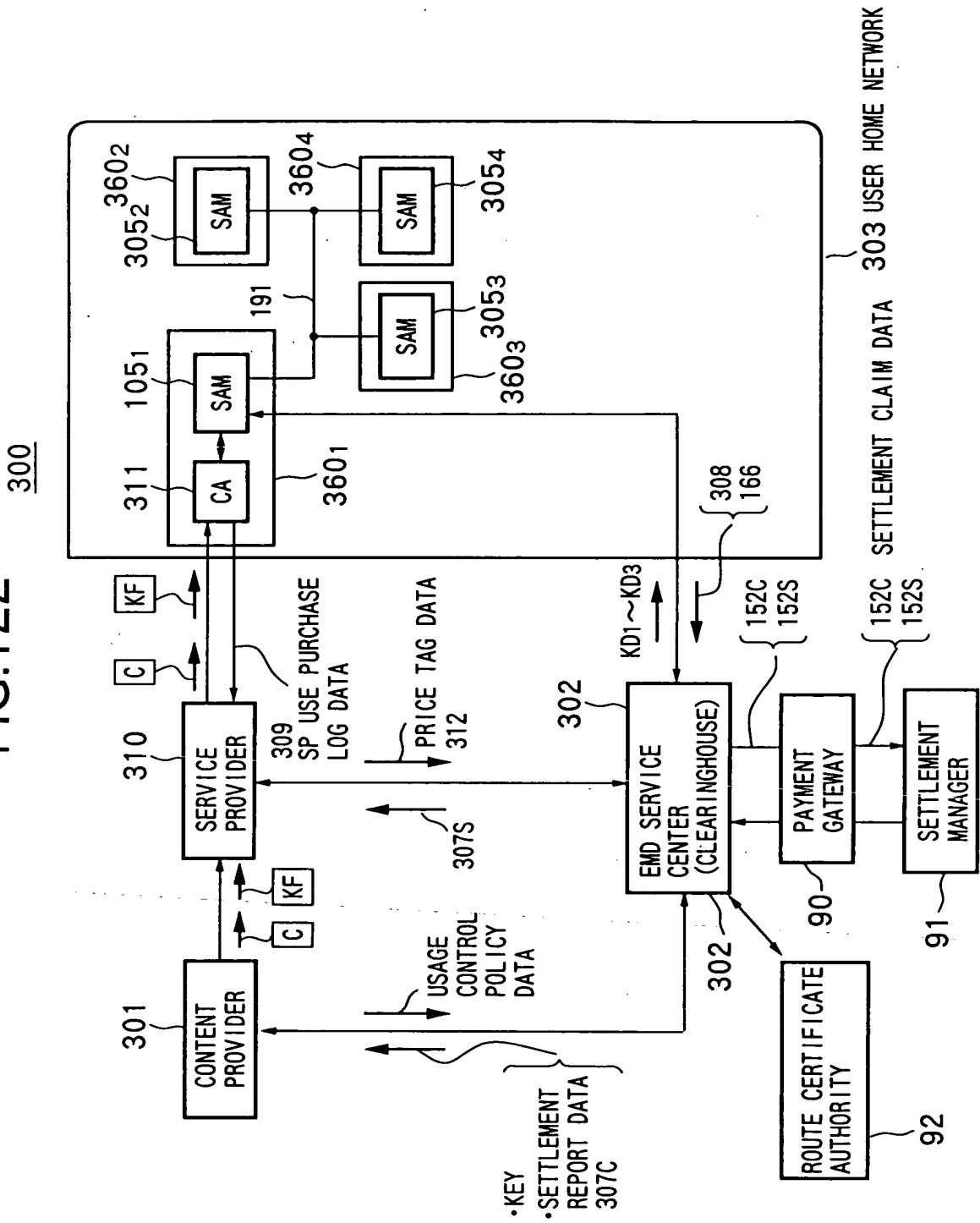
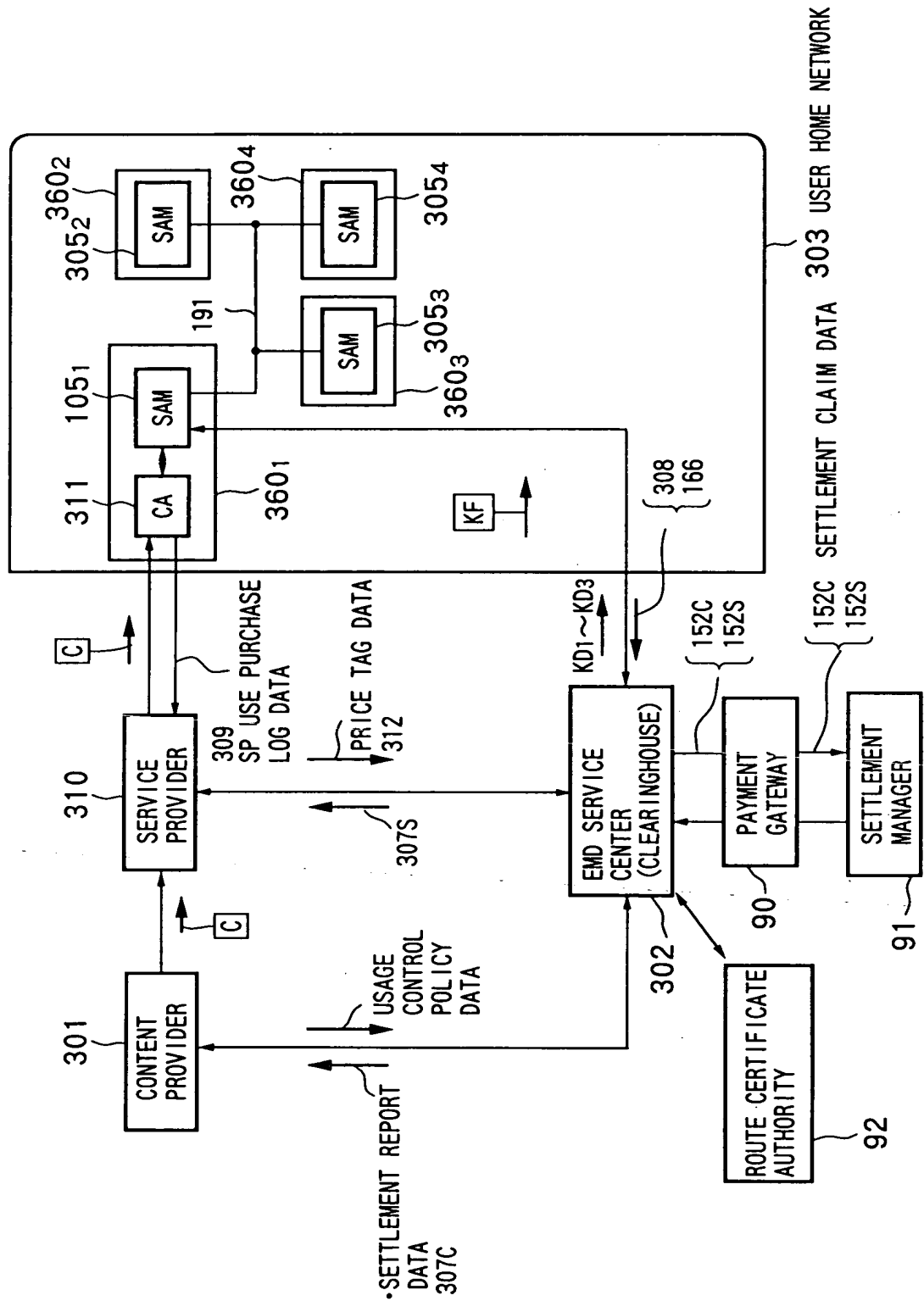
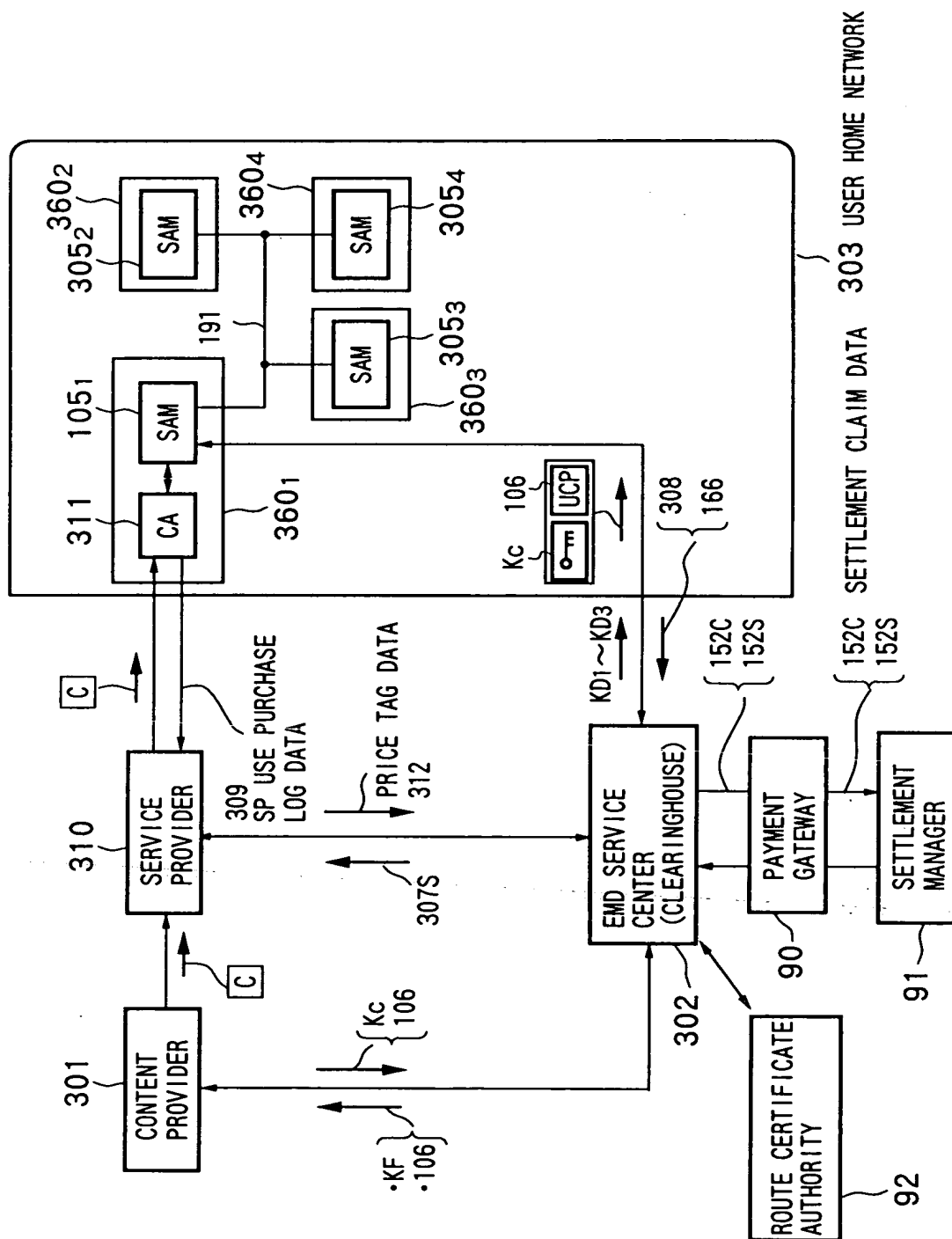


FIG. 123



300



300

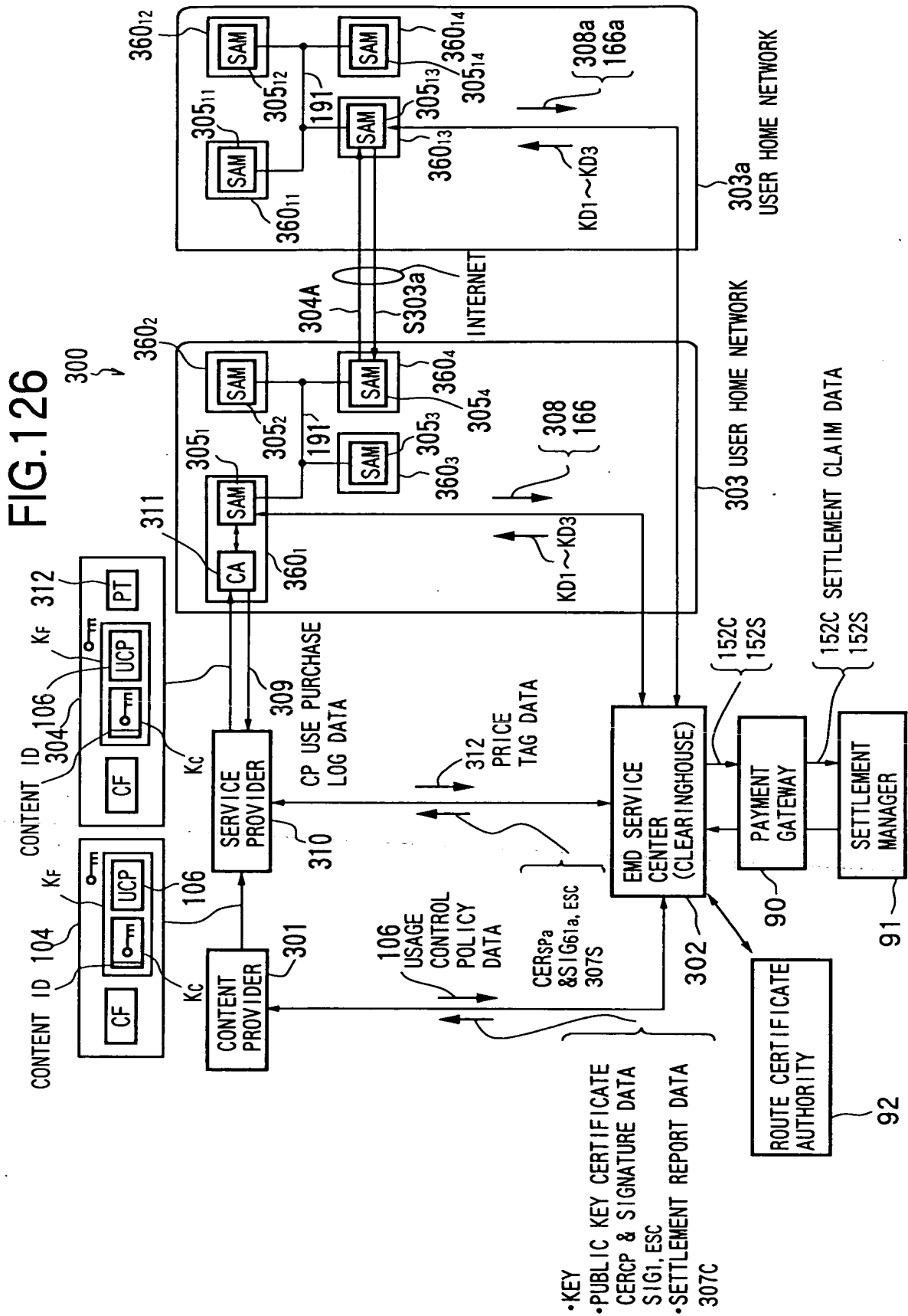


FIG.127

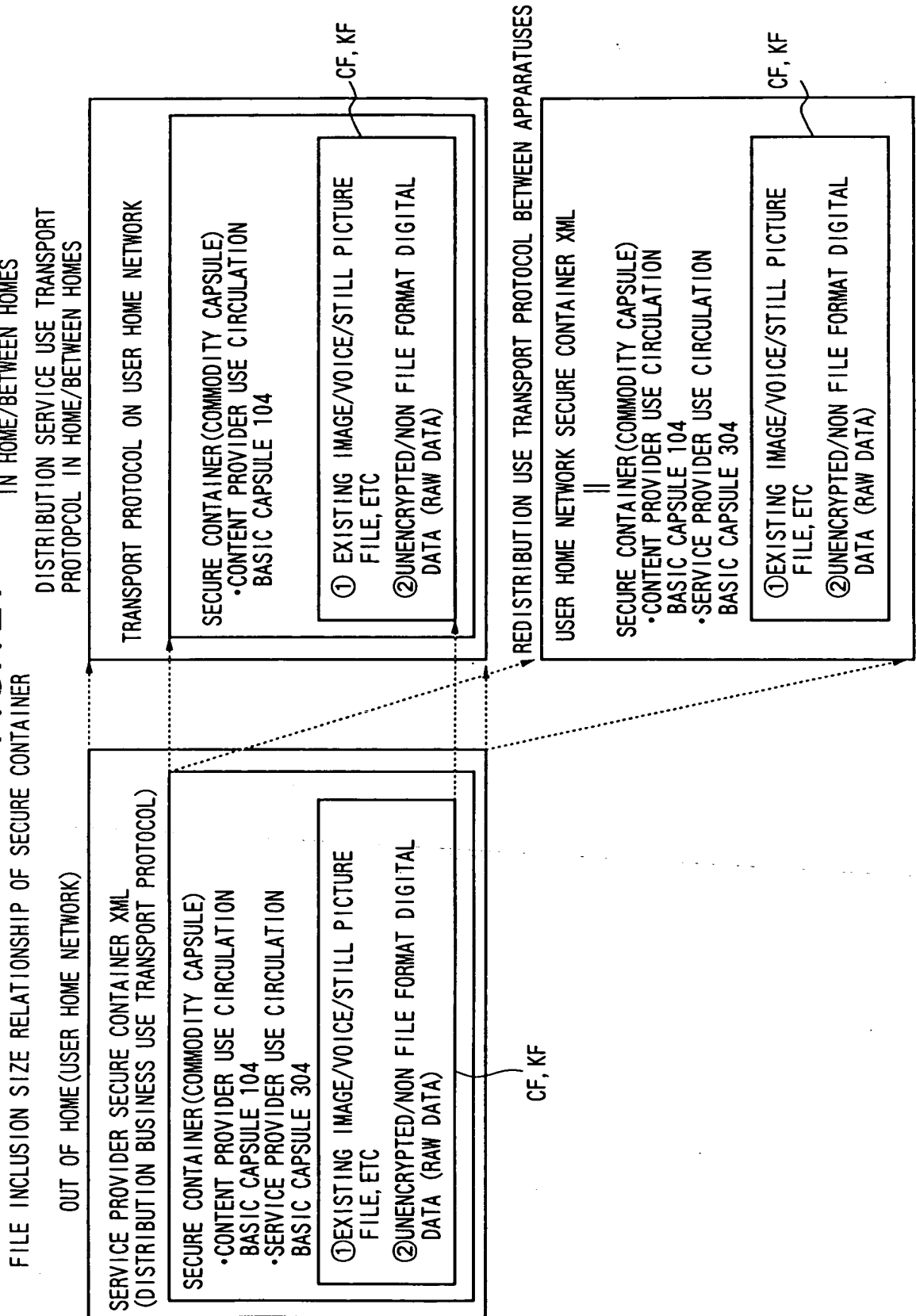


FIG. 128

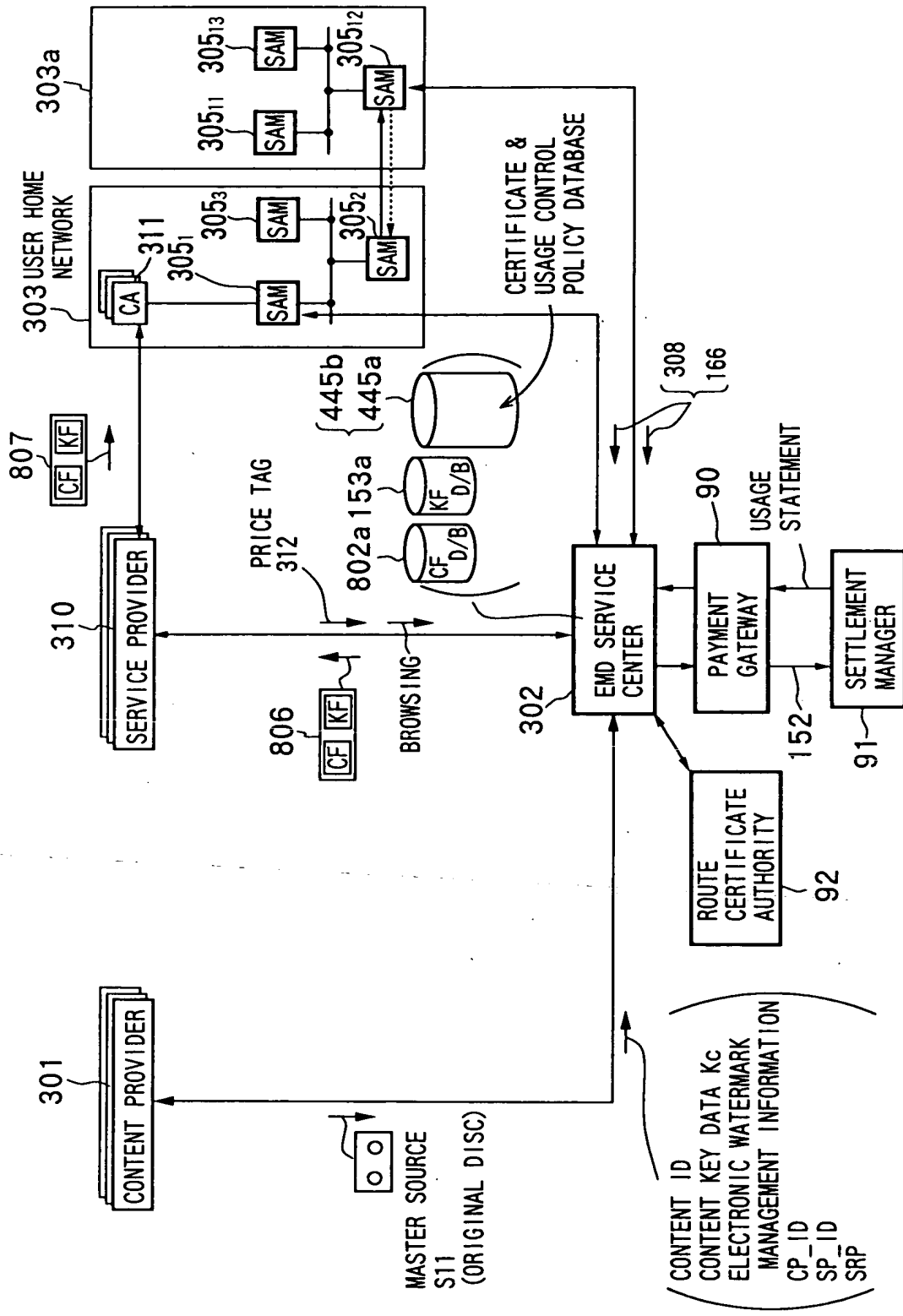


FIG.129

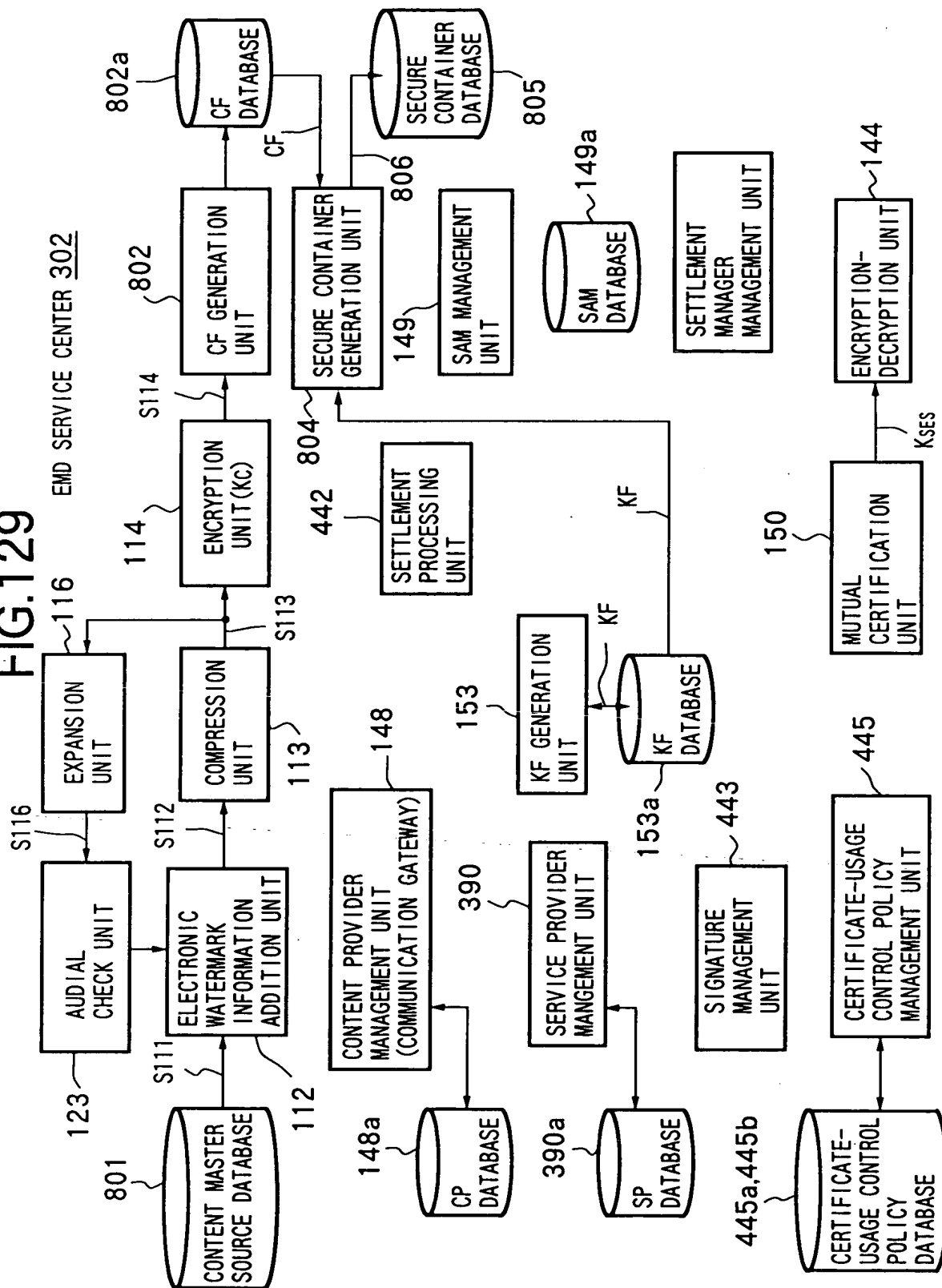


FIG. 131

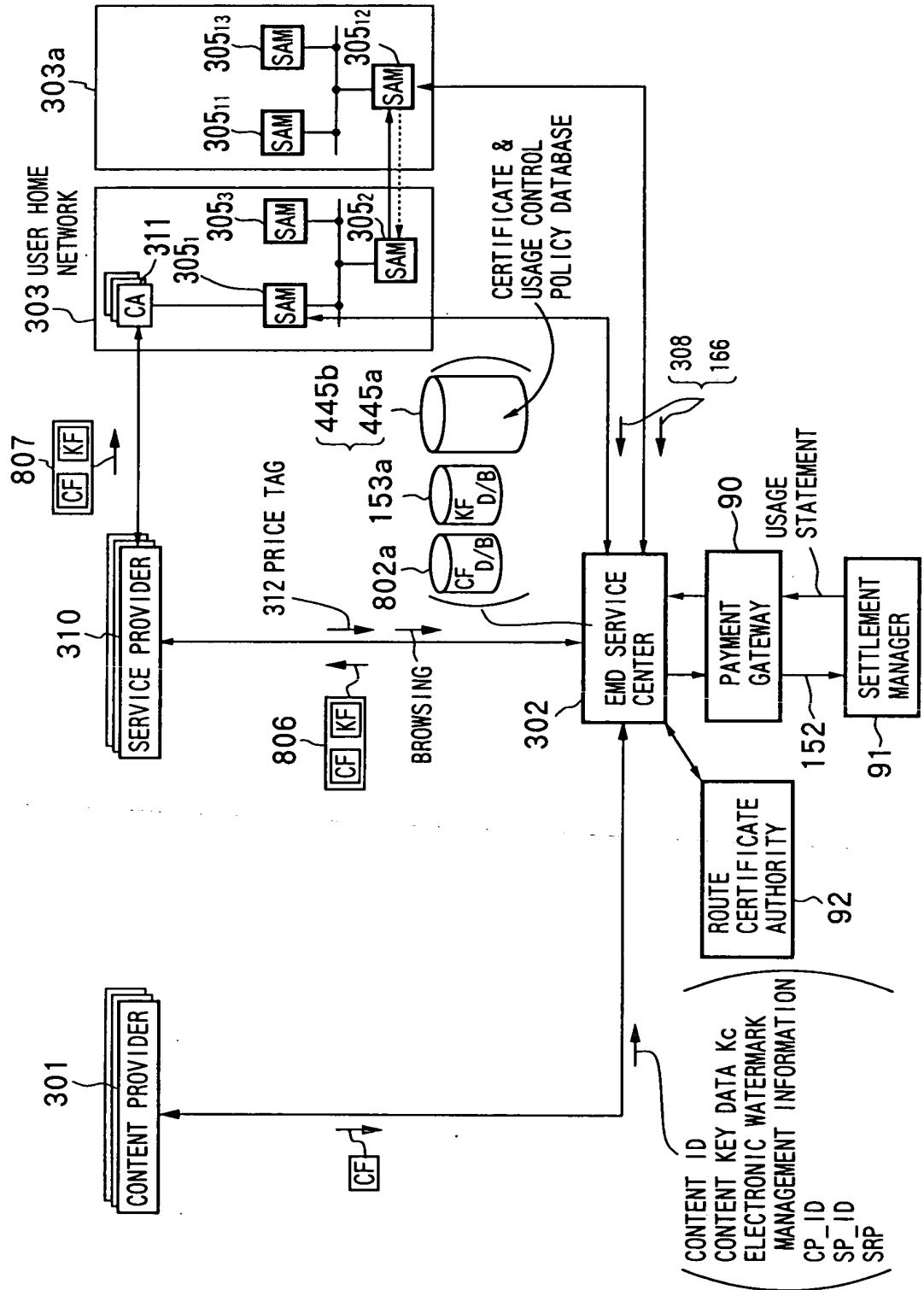


FIG. 132

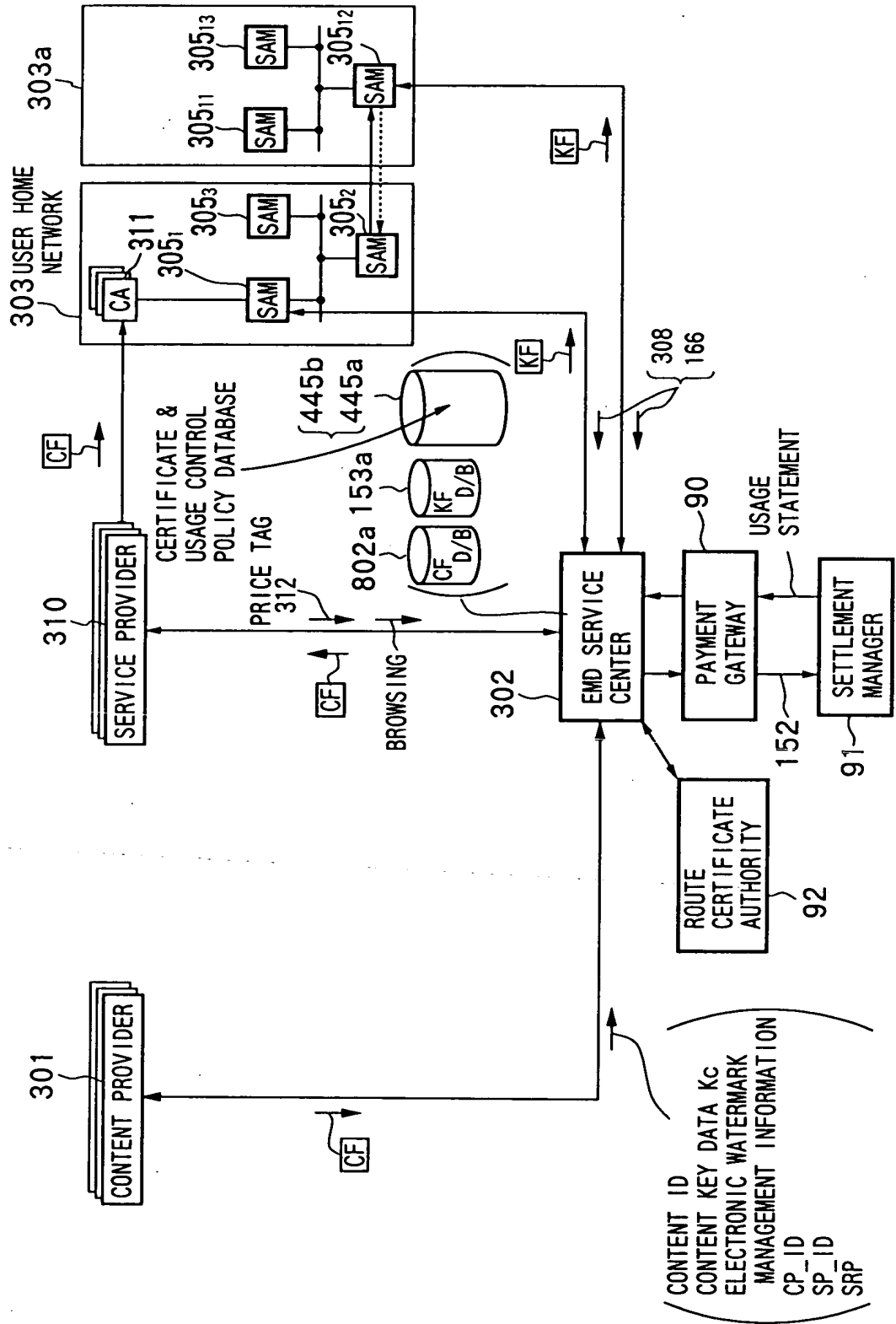


FIG. 133

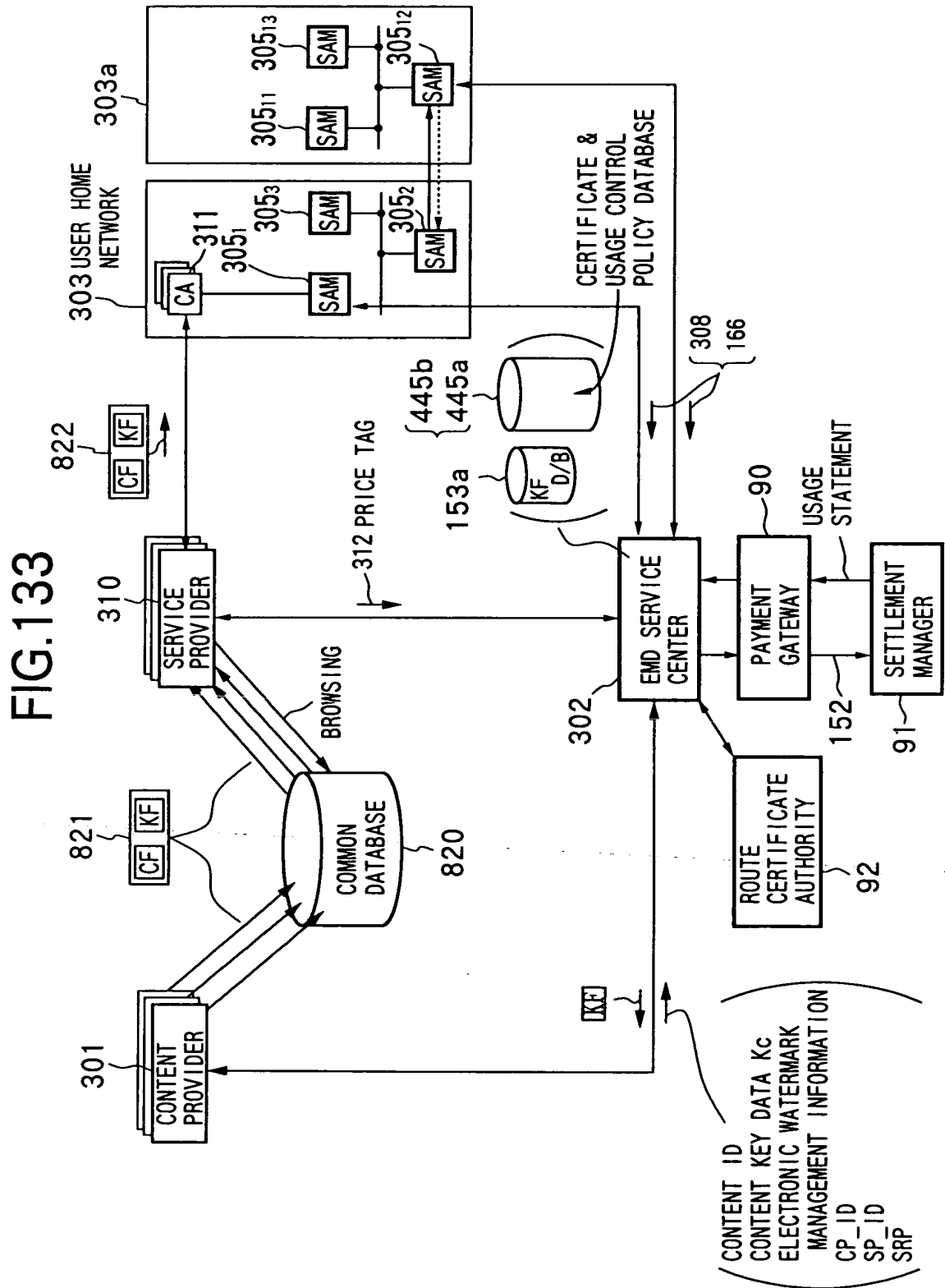
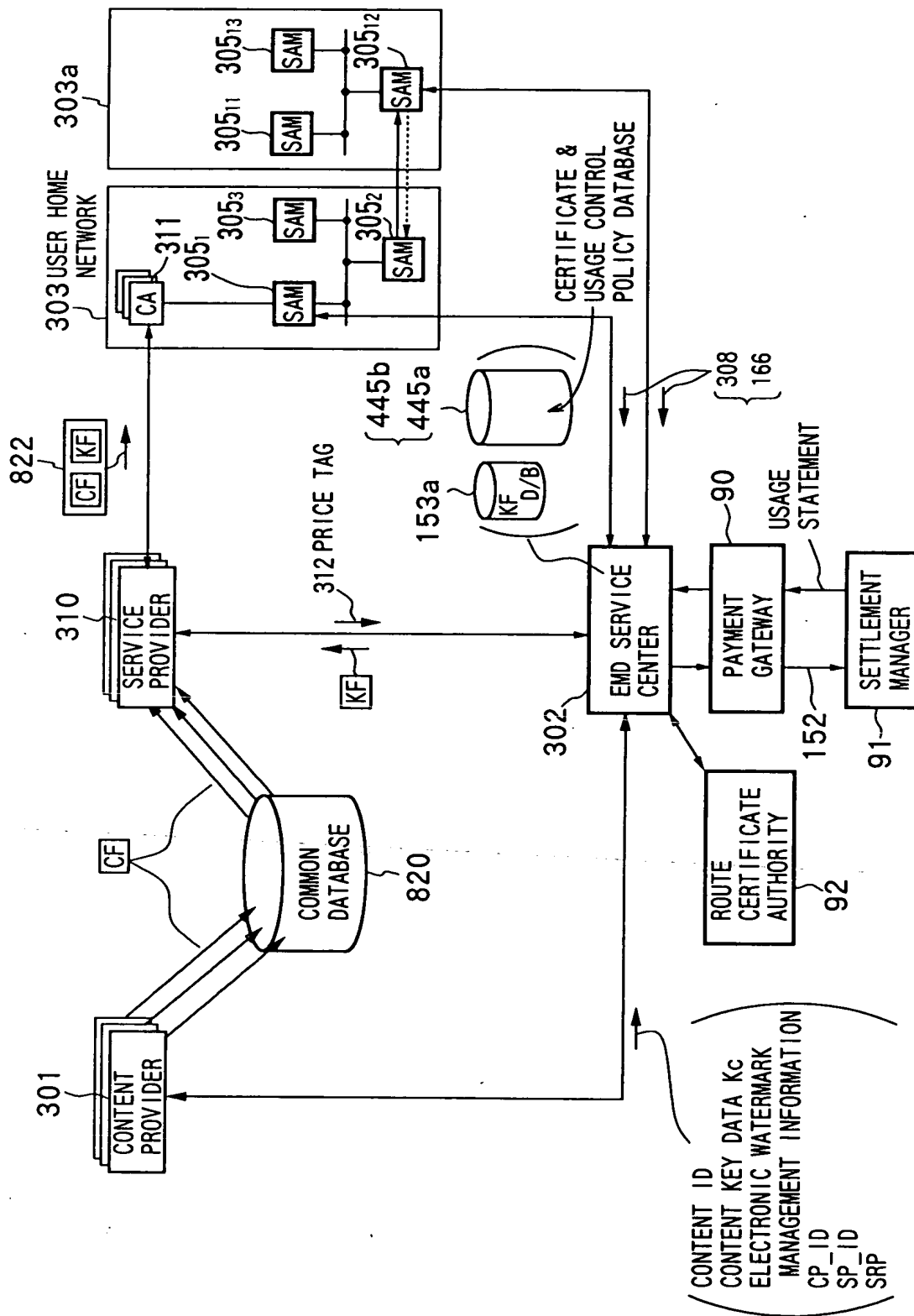


FIG. 134



100

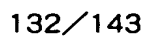
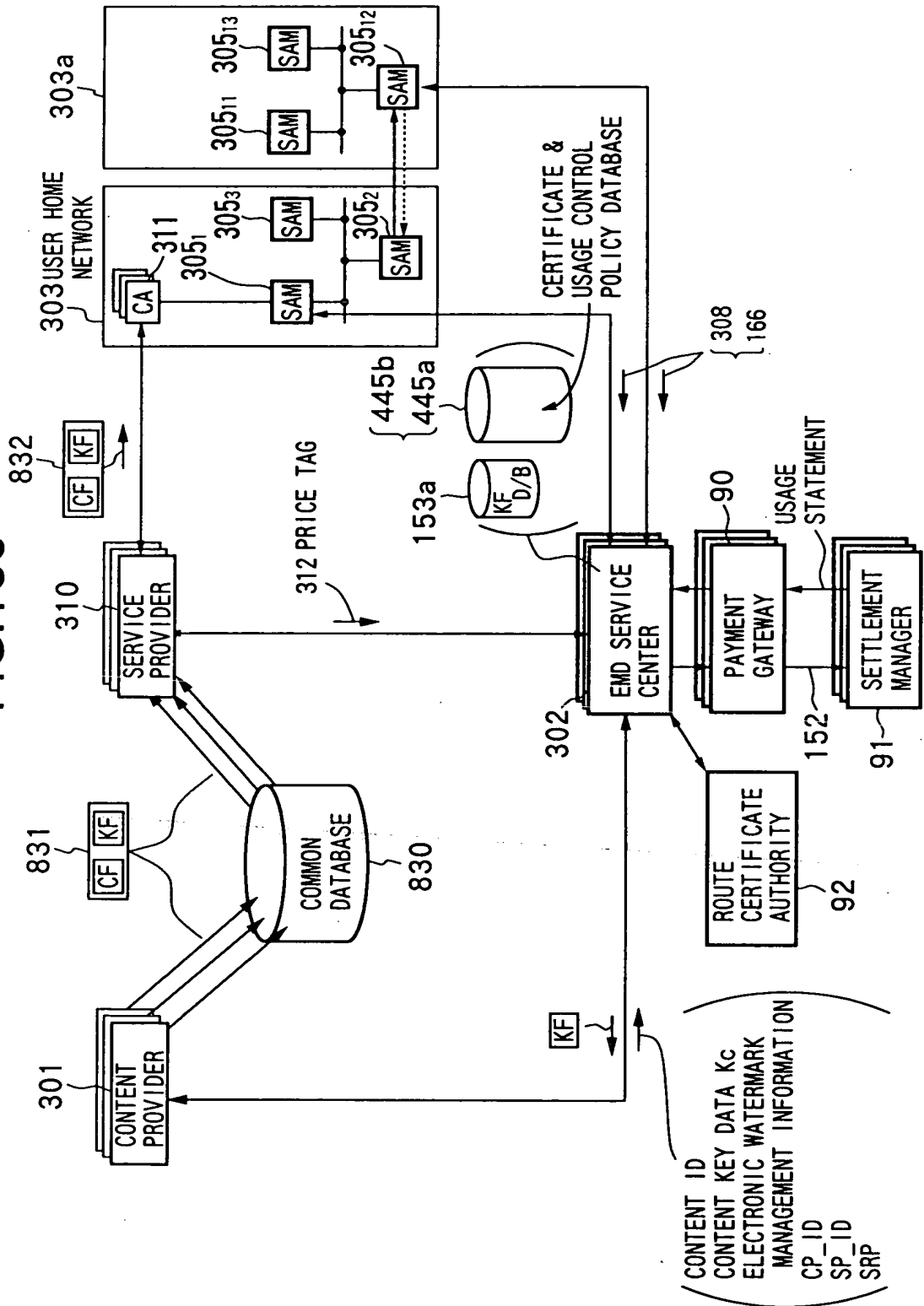
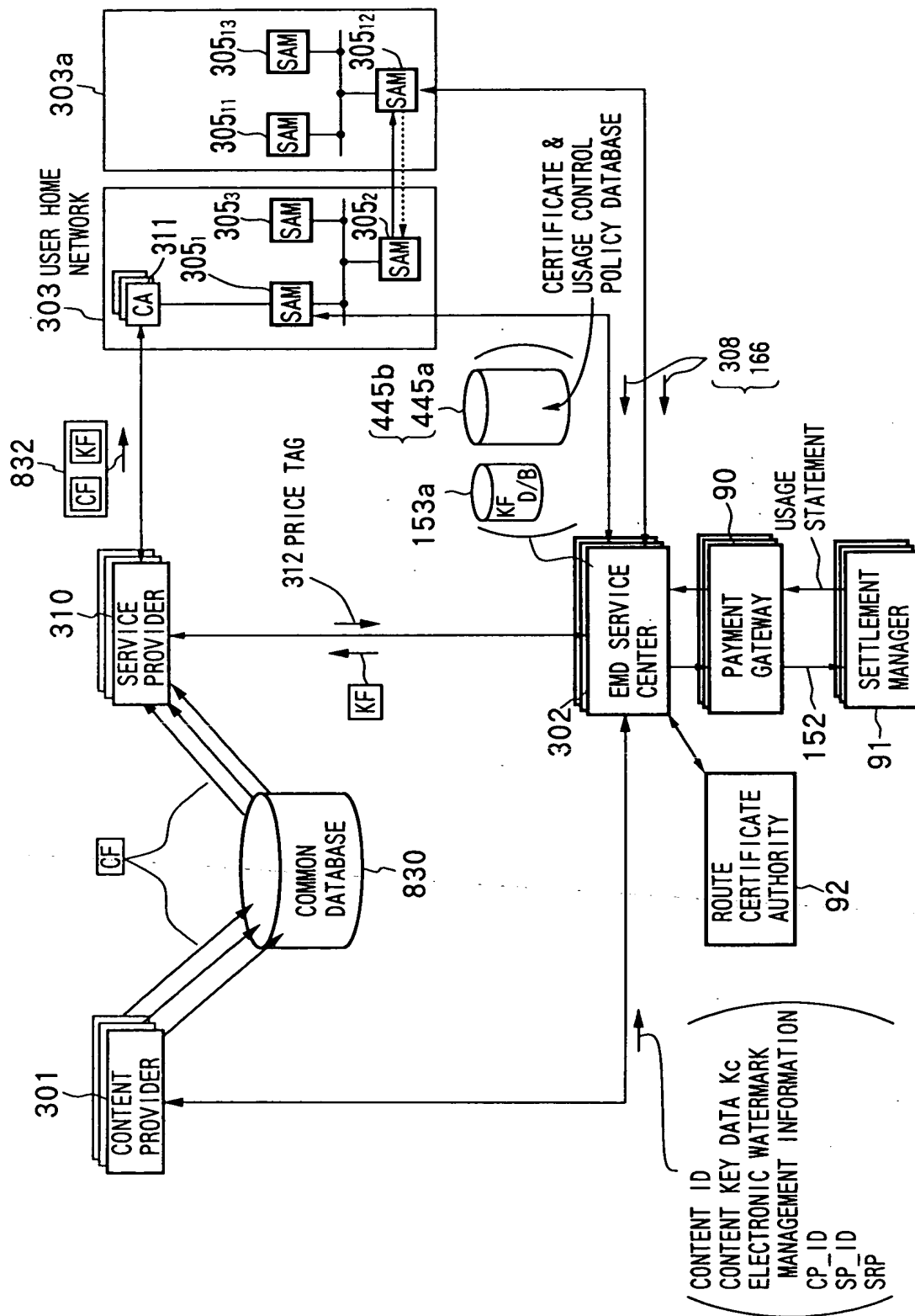
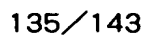


FIG. 136

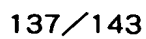


134/143



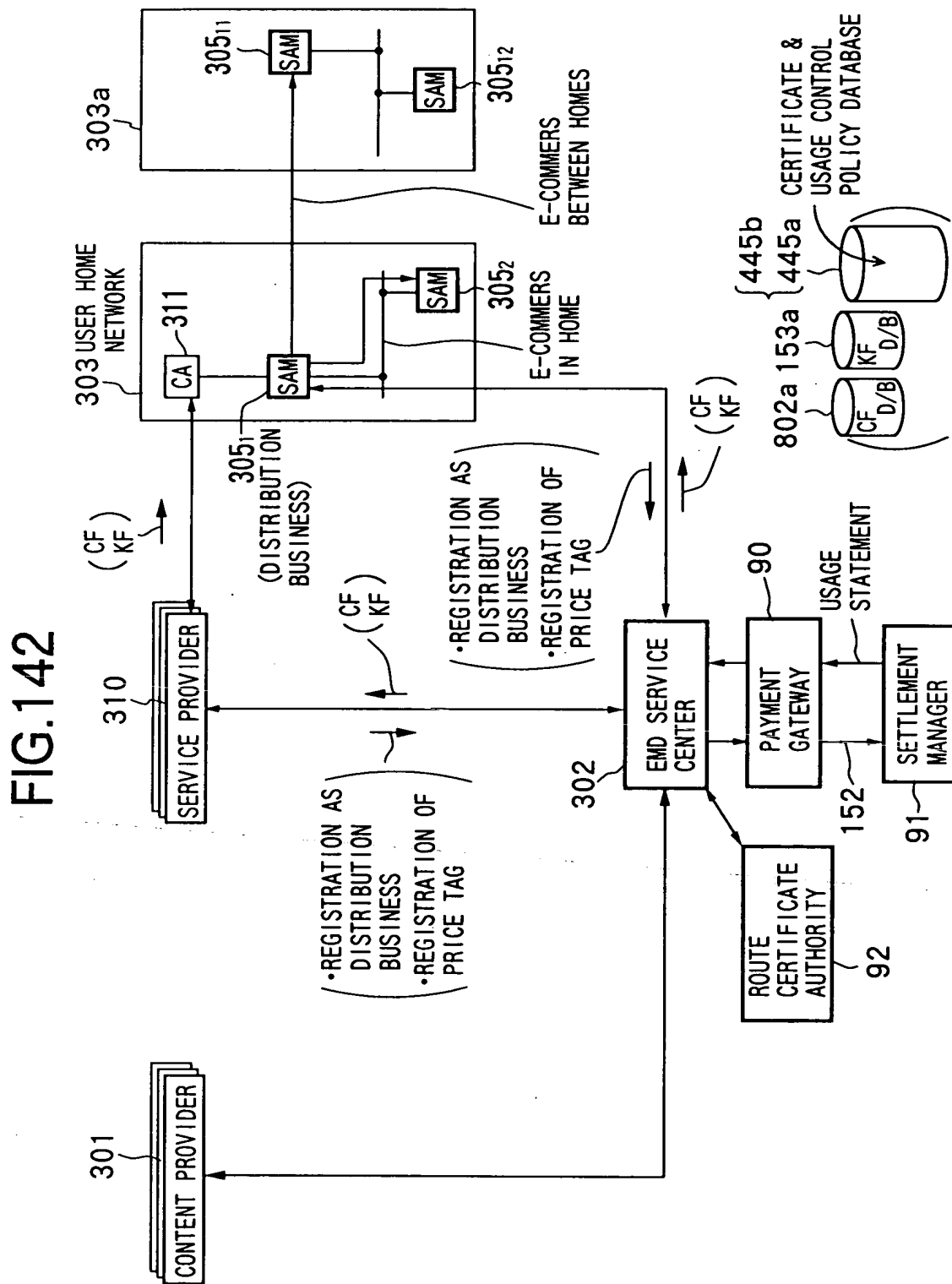


[illegible]



1000





140/143

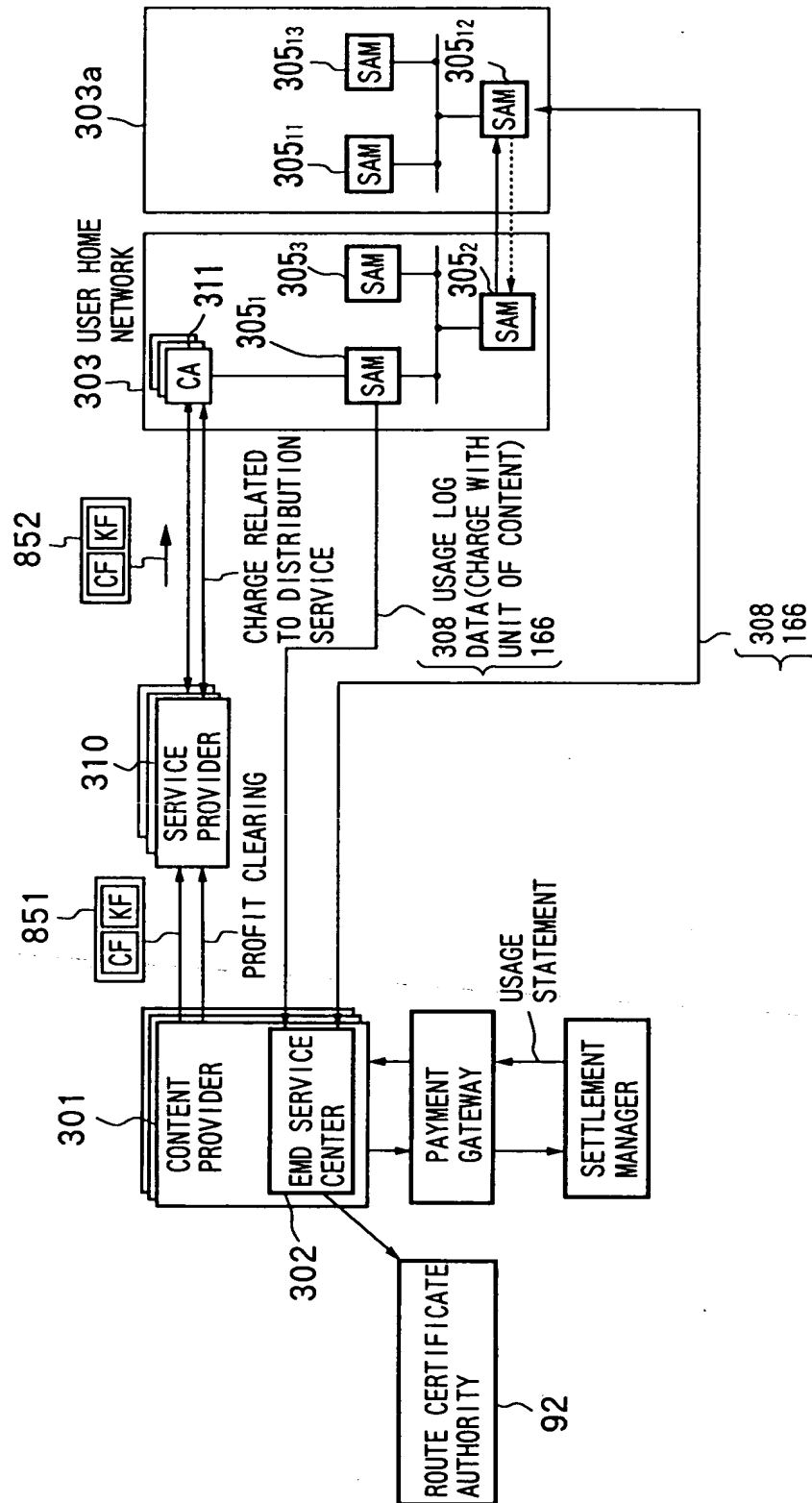
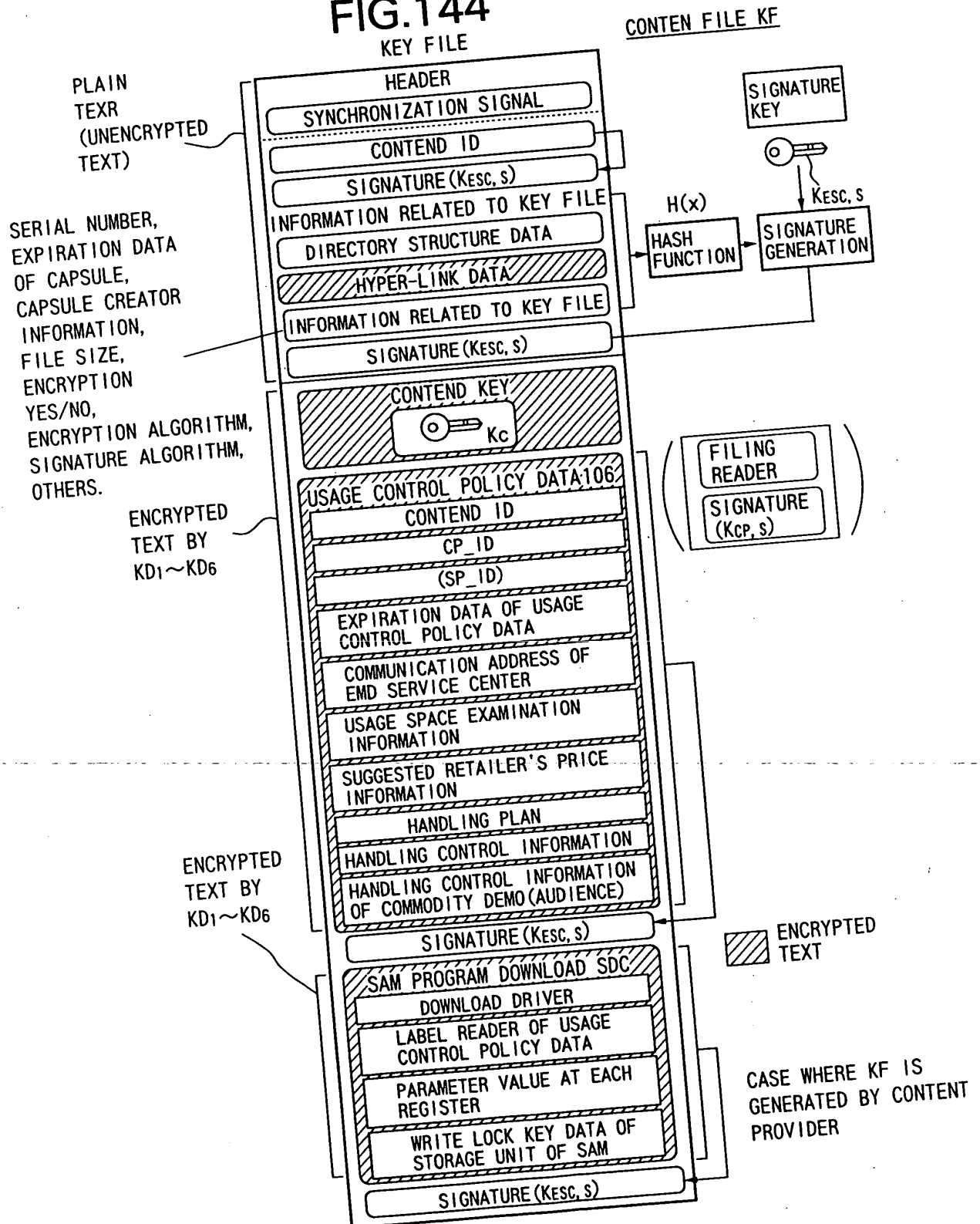
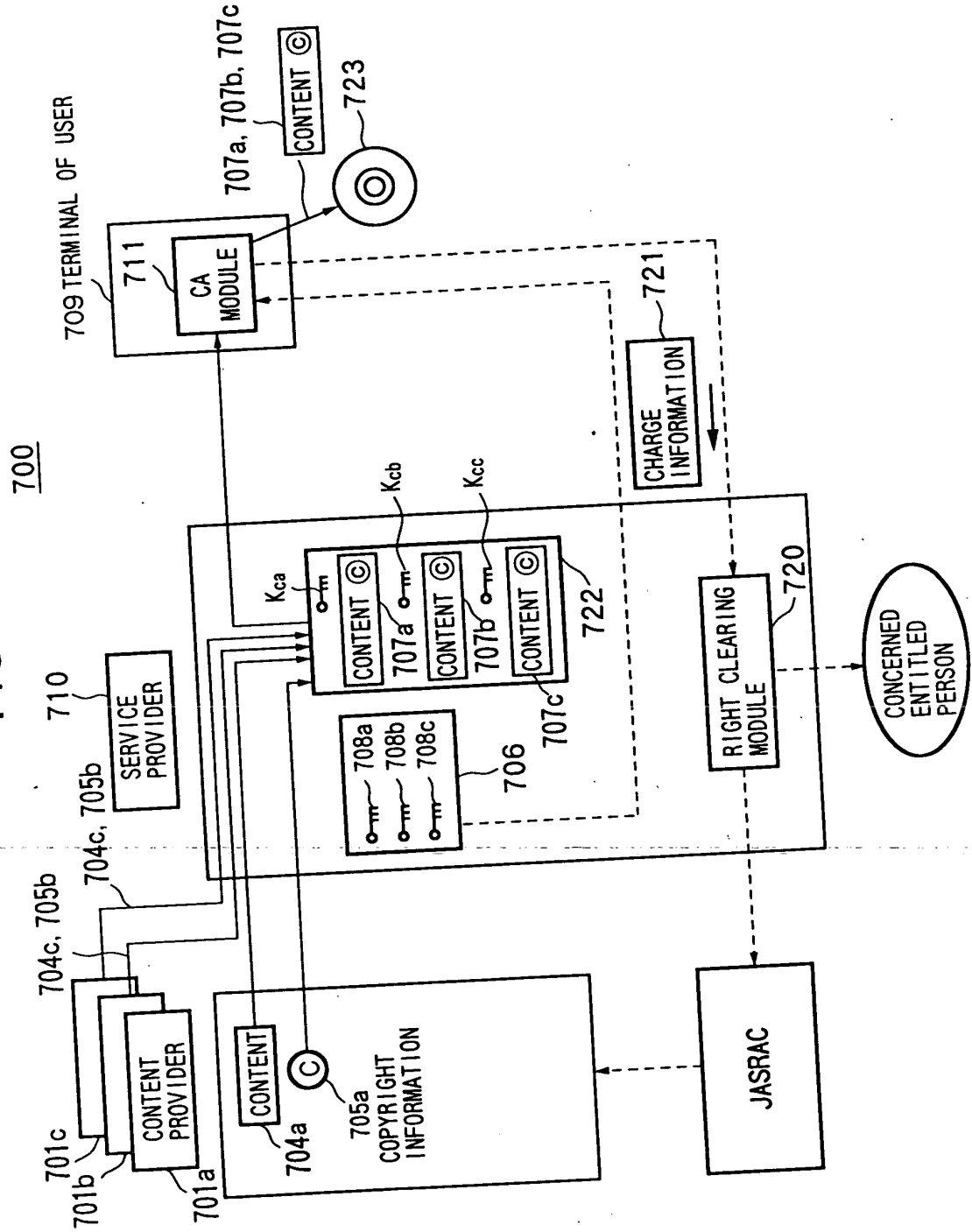


FIG.144



09856276-100201



LIST OF REFERENCE NUMERALS

90... payment gateway
91... settlement manager
92... route certificate authority
100, 300... EMD system
101, 301... content provider
102, 302... EMD service center
103, 303... user home network
104, 304... secure container
105₁ to 105₄, 305₁ to 305₄... SAM
106... usage control policy data
107, 307... settlement report data
108, 308... usage log data
160₁... network apparatus
160₂ to 160₄... AV apparatuses
152, 152c, 152s... settlement claim data
191... bus
310... service provider
311... CA module
312... price tag data
CF... content file
KF... key file
Kc... content key data